



Enterprise IP Solutions

OfficeServ 7400

GSIM User Manual

Every effort has been made to eliminate errors and ambiguities in the information contained in this guide. Any questions concerning information presented here should be directed to SAMSUNG TELECOMMUNICATIONS AMERICA, 1301 E. Lookout Dr. Richardson, TX. 75082 telephone (972) 761-7300. SAMSUNG TELECOMMUNICATIONS AMERICA disclaims all liabilities for damages arising from the erroneous interpretation or use of information presented in this guide.

Samsung Telecommunications

Publication Information

SAMSUNG TELECOMMUNICATIONS AMERICA reserves the right without prior notice to revise information in this publication for any reason. SAMSUNG TELECOMMUNICATIONS AMERICA also reserves the right without prior notice to make changes in design or components of equipment as engineering and manufacturing may warrant.

Copyright 2006

Samsung Telecommunications America

All rights reserved. No part of this manual may be reproduced in any form or by any means—graphic, electronic or mechanical, including recording, taping, photocopying or information retrieval systems—without express written permission of the publisher of this material.

Trademarks

Enterprise IP Solutions

OfficeServ™ is a trademark of SAMSUNG Telecommunications America, L.P.
WINDOWS 95/98/XP/2000 are trademarks of Microsoft Corporation.

PRINTED IN USA

INTRODUCTION

Purpose

This document introduces the OfficeServ 7400 GSIM, an application module of the OfficeServ 7400, and describes procedures on installing and using the software.

Document Content and Organization

This document consists of three chapters and abbreviation, which are summarized as follows:

CHAPTER 1. Overview of OfficeServ 7400 GSIM

This chapter briefly introduces the OfficeServ 7400 GSIM.

CHAPTER 2. Instalng of OfficeServ 7400 GSIM

This chapter describes the installation procedure and login procedure.

CHAPTER 3. Using OfficeServ 7400 GSIM

This chapter describes how to use the menus of the OfficeServ 7400 GSIM.

ABBREVIATIONS

Abbreviations frequently used in this document are described.

Conventions

The following types of paragraphs contain special information that must be carefully read and thoroughly understood. Such information may or may not be enclosed in a rectangular box, separating it from the main text, but is always preceded by an icon and/or a bold title.



WARNING

Provides information or instructions that the reader should follow in order to avoid personal injury or fatality.



CAUTION

Provides information or instructions that the reader should follow in order to avoid a service failure or damage to the system.



CHECKPOINT

Provides the operator with checkpoints for stable system operation.



NOTE

Indicates additional information as a reference.

Console Screen Output

- The lined box with ‘**Courier New**’ font will be used to distinguish between the main content and console output screen text.
- ‘**Bold Courier New**’ font will indicate the value entered by the operator on the console screen.

References

OfficeServ 7400 General Description

OfficeServ 7400 System Description introduces OfficeServ 7400 and describes the system information necessary for the understanding of this system, such as hardware configuration, specification, and functions.

OfficeServ 7400 Installation Manual

OfficeServ 7400 Installation Manual describes the conditions necessary for the installation of the system and how to inspect and operate the system.

OfficeServ 7400 Programming Manual

The OfficeServ 7400 Call Server Programming Manual describes the method of using the Man Machine Communication (MMC) program that changes system settings by using phones.

Revision History

EDITION	DATE OF ISSUE	REMARKS
01	05.2006	Initial Release

SAFETY CONCERNS

In order to ensure product safety and proper operation, information followed by the following icons should be carefully read before installing or using the product:

Symbols



Caution

Indication of a general caution.



Restriction

Indication for prohibiting an action for a product.



Instruction

Indication for commanding a specifically required action.



CAUTION



When Changing Network Interface

Note that all IP sessions in working are disconnected for a while if network interface(IP, Gateway, and Subnet Mask) is changed and finally applied during the router operation.



When Using a Web Browser

Use Microsoft Internet Explorer(version 6.0 or higher) as the web browser for the manitenance of GSIM. Other web browsers are not supported.



When Changing DB

If DB is changed in OfficeServ 7400 GSIM, the system restarts.



When Using a Private key

The private key is provided with the package. The private key allows accessing SSH from the outside. Thus, only trusted administrator should use the key.



When Deleting Internet Temporary Files

If GSIM package is upgraded, Internet temporary files should be deleted. Select **[Internet Explorer] → [Tools] → [Internet Options]** menu and click the **[Delete Cookies]** and the **[Delete Files]** buttons in **[Internet Temporary Files]** area. If these files is not deleted, the webscreen of GSIM may not be normally displayed.

TABLE OF CONTENTS

INTRODUCTION	I
Purpose	I
Document Content and Organization.....	I
Conventions.....	II
Console Screen Output	II
References	III
Revision History.....	III
SAFETY CONCERNS	IV
Symbols.....	IV
Caution	V
CHAPTER 1. Overview of OfficeServ 7400 GSIM	1
Introduction to OfficeServ 7400	1
Introduction to OfficeServ 7400 GSIM	2
CHAPTER 2. Installation of OfficeServ 7400 GSIM	4
Software Installation.....	4
Getting Started.....	6
CHAPTER 3. Using OfficeServ 7400 GSIM	8
Port Menu	9
PORT	10
VLAN	13
Layer2 Menu.....	17
RSTP	18
Port Trunking	22
GVRP	25
IGMP Snooping	28
Authentication.....	31

Interface	33
IP Configuration	33
DNS	34
Status.....	34
Utility.....	35
Layer 3 Menu.....	37
General	38
Configuration	39
List	46
Status.....	52
IPMC	55
General	56
Configuration	57
Status.....	63
QoS Menu.....	66
Ingress Service	66
Egress Service.....	75
Application Menu.....	77
VoIP Service Menu	78
DHCP Server	80
DHCP Relay Agent	82
System Menu	84
DB Config	85
Admin Config	85
Log.....	87
NTP Server	89
Upgrade.....	91
Appl Server	91
Reboot	92
Management Menu	93
SNMP	93
RMON.....	96

ABBREVIATION**99**

A - L	99
N-V	100

CHAPTER 1. Overview of OfficeServ 7400 GSIM

This chapter introduces OfficeServ 7400 system and OfficeServ 7400 GSIM.

Introduction to OfficeServ 7400

The OfficeServ 7400 is a single platform that delivers the convergence of voice, data, wired and wireless communications for small and medium offices. The ‘office in a box’ solution offers TDM voice processing, voice over IP integration, wireless communications, voice mail, computer telephony integration, data router and switching functions, all in one powerful platform.

With the GWIM, GPLIM and GSIM modules, the OfficeServ 7400 provides network functions such as a gigabit switching, Power Over Ethernet, high speed data routing, and network security in a single converged solution.

This document describes the data and routing capabilities of OfficeServ 7400 GSM.



NOTE

Structure of OfficeServ 7400

For the information on the structure, features, or specifications of the OfficeServ 7400, refer to [‘OfficeServ 7400 General Description’](#).

Introduction to OfficeServ 7400 GSIM

OfficeServ 7400 provides the following functions via GSIM based on IP:

Switch Functions

- L2/L3 Switch Function
- Jumbo Packet(9216 Bytes) Support
- Managed Switch functions
- Learning Bridge function using Spanning-Tree algorithm
- Layer 2 Frame Priority function (802.1p)
- 802.3x Layer 2 Flow Control
- Packet Mirroring function
- Virtual VLAN(VLAN) function(on the basis of ports, 802.1Q tag)
- VLAN Classification(MAC Based/IP Based/Protocol Based) Function
- Ingress Filtering function for 802.1q VLAN Security
- Dynamic VLAN Management function via GARP VLAN Registration Protocol(GVRP) function
- IP Multicasting Relay support(IGMP Snooping function)
- Load Sharing function for Link Aggregation Control Protocol(LACP)/Port Trunking

Router Functions

- Path management and queuing function of data packets for external WAN and internal LAN
- Static and dynamic routing functions
 - Support of Routing Information Protocol version1(RIPv1), RIPv2, Open Shortest Path First version2(OSPFv2),and Border Gateway Protocol4(BGP4) routing protocol
- Dynamic Host Configuration Protocol(DHCP) function in Ethernet WAN interface
- Support of IP Multicasting
 - Support of Internet Group Management Protocol version1(IGMPv1) and IGMPv2 protocol
 - Support of Distance Vector Multicast Routing Protocol(DVMRP) and Protocol Independent Multicast-Sparse Mode(PIM-SM) Multicast Route Protocol

Data Network Application Functions

- DHCP Server function
 - Auto-set of network environment for IP equipment in another function block of the OfficeServ 7400 system
- DHCP Relay function
 - Connection of IP equipment in another function block of the OfficeServ 7400 system to an external DHCP server to enable to automatically set network environment.

QoS Functions

- Priority process for layer 2 frame under 802.1p standard(Switch function)
- Priority queuing process for layer 3 packets and priority queuing for a specified IP.
- Priority queuing process for layer 4 packets and priority for Real-time Transport Protocol(RTP) packets(UDP/TCP port)

Management Functions

- Configuration and verification functions for the operations of GSIM functional block via a browser
- Configuration and verification functions for the operations of GSIM functional block via the Simple Network Management Protocol(SNMP)
- 4-Real-time Monitoring(4RMON) function
- System monitoring and management via the system log function
- System synchronization function via Network Time Protocol(NTP)
- Program Upgrade
 - Program upgrade via TFTP
 - Program upgrade via HTTP
 - Program upgrade via Local manager's PC

CHAPTER 2. Installation of OfficeServ 7400 GSIM

This chapter describes the installation and the login procedure for OfficeServ 7400 GSIM.

Software Installation

OfficeServ 7400 software is installed on GWIM board. The software package is composed of items described below:

Package	File	Description
Bootrom Package	gsim-bootldr.img-vx.xx	Boot ROM program
	gsim-bootldr.img-vx.xx.sum	
Main Package	gsim-pkg-vx.xx.tar.gz	Upgrade package for HTTP
	gsim-os..img-vx.xx	'os' partition upgrade package for TFTP
	gsim-firmware.img-vx.xx	'Firmware' partition upgrade package for TFTP
	gsim-configdb.img-vx.xx	'configdb' partition upgrade package for TFTP
	gsim-logdb.img-vx.xx	'logdb' partition upgrade package for TFTP
	gsim-flash1.img-vx.xx gsim-flash1.img-vx.xx.sum	Fusing file for the first flash memory
	gsim-flash2.img-vx.xx gsim-flash2.img-vx.xx.sum	Fusing file for the second flash memory

GWIM Installation

Configure the environment as follows to access GSIM.

1. Insert the GSIM into an open slot in the OfficeServ 7400 cabinet.
2. Connect a PC to any of the Gigabit ethernet ports on the GSIM board.
3. Run Internet Explorer from the PC and access the initial IP (10.0.3.1) of GSIM. The default IP address of the GSIM is set to 10.0.3.1/24.



Caution for the Use of a Web Browser

The version of the Internet Explorer should be 6.0 or higher for the maintenance of GSIM. Other web browsers are not supported.



Caution for the initial Use of the System

The time setup of the system should be performed before the system is used initially. If not, the system may be malfunctioned.

Getting Started

The start procedure of OfficeServ 7400 GSIM is as follows:

1. Start Internet Explorer and enter the IP address of the GSIM into the address bar. The login window shown below will appear:

SAMSUNG

Enterprise IP Solutions
OfficeServ 7400
OfficeServ 7400 is enterprise IP solutions made by Samsung Electronics. It provides integrated solutions for you.

✉ 📞 📠 📧

Login

ID

Password

▶ Save Your ID? ☐

▶ Forget Your ID & Password?

Copyright © 2003 Samsung Electronics Co., Ltd V1.0

2. Log in using the administrator ID and password. The following window will appear. GSIM menus are displayed in the upper part of the screens. Select each menu to display its submenus on the left section of the screen. For more detailed information for each menu, refer to ‘Chapter 3. Using OfficeServ 7400 GSIM’ of this document.

(The default administrator name is “**admin**” and the default password is “**root**”)

OfficeServ 7400 GSIM

Administrator Port | Layer2 | Interface | Layer3 | IPMC | QoS | Application | System | Management

Port Configuration

Port	TGID	Active	Auto Negotiation	Jumbo	Flow Ctrl TX	Flow Ctrl RX	Storm Ctrl Bcast	Storm Ctrl Mcast	Storm Ctrl DLF
ALL	-	☐	Auto	☐	☐	☐			
Port1	-	☒	Auto	☐	☐	☐			
Port2	-	☒	Auto	☐	☐	☐			
Port3	-	☒	Auto	☐	☐	☐			
Port4	-	☒	Auto	☐	☐	☐			
Port5	-	☒	Auto	☐	☐	☐			
Port6	-	☒	Auto	☐	☐	☐			
Port7	-	☒	Auto	☐	☐	☐			
Port8	-	☒	Auto	☐	☐	☐			
Port9	-	☒	Auto	☐	☐	☐			
Port10	-	☒	Auto	☐	☐	☐			

OK Reset

Save Configuration

3. Click the **[Logout]** button on the upper section of the screen to close the connection to the GSIM system.

CHAPTER 3. Using OfficeServ 7400 GSIM

This chapter describes how to use the menus of OfficeServ 7400 GSIM.

The configuration of OfficeServ 7400 GSIM menus is as follows:

Port	Layer2	Interface	Layer3	IPMC
Port Port Config. Statistics Mirror Config. Forward Table VLAN Configuration Status	RSTP Configuration Status Port Trunking Configuration Status GVRP Configuration Status IGMP Snooping Time Interval Function Multicast Filter Forwarding Table Management Authentication Configuration Management	IP Configuration DNS Status Utility Ping	General Routes Management Configuration Static RIP RIP Interface OSPF OSPF Interface BGP List Access List Prefix List Route Map As Path List Community List Key Chain Status RIP OSPF BGP	General Mroutes Management Configuration IGMP DVMRP DVMRP Intf PIM-SM PIM-SM Intf Status IGMP Groups DVMRP PIM-SM
QoS	Application	System	Management	
Ingress Service Class Map Policy Map Service Map Egress Service Schedule mode CoS mapping	VoIP Service Management VoIP DB DHCP Server Configuration Management Lease Info DHCP Relay Agent Configuration Management	DB Config Admin Config Log Configuration Report Download Time Config NTP Config Manual Config Timezone Upgrade Appl Server Reboot	SNMP Configuration Status Management RMON Configuration Status Management	

Port Menu

Select the **[Port]** menu. The submenus will be displayed in the upper left side of the window as follows.

Network	Port
Network Ethernet0 Ethernet1 Ethernet2 Serial0 (V.35) Serial1 (HSSI) DNS Network Link ARP Network Status	Port Port Config. Statistics Mirror Config. Forward Table VLAN Configuration Status

Menu	Sub-menu	Description
Port	Port Config.	Display general port configurations
	Statistics	Displays the statistic information of the port.
	Mirror Config.	Displays the information on the port mirroring configuration.
	Forward Table	Displays the MAC Table information learned on each port.
VLAN	Configuration	Sets the VLAN configuration.
	Status	Displays the information configured in [VLAN] → [Configuration] menu.

PORT

Port Config.

[Port] → [Port Config]

To apply the data specified to the system, press the **[OK]** button.

To cancel the newly configured data, press the **[Cancel]** button.

Port Configuration

The Port Configuration window is used for the general configuration of each port.

Port Configuration									
Port	TGID	Active	Auto Negotiation	Jumbo	Flow Ctrl		Storm Ctrl(pps)		
					TX	RX	Bcast	Mcast	DLF
ALL	-	☐	Auto	☐	☐	☐			
Port1	-	☒	Auto	☐	☐	☐			
Port2	-	☒	Auto	☐	☐	☐			
Port3	-	☒	Auto	☐	☐	☐			
Port4	-	☒	Auto	☐	☐	☐			
*Port5	1	☒	Auto	☐	☐	☐			
*Port6	1	☒	Auto	☐	☐	☐			
Port7	-	☒	Auto	☐	☐	☐			
Port8	-	☒	Auto	☐	☐	☐			
Port9	-	☒	Auto	☐	☐	☐			
Port10	-	☒	Auto	☐	☐	☐			
Sa1	-	☒	Auto	☐	☐	☐			

Categories	Description
Port	Displays the port to be configured. If a port name begins with '*', it indicates that the port is a Trunk/LACP member port. The contents such as 'Sa*' or 'Po*' (TGID is included in *) that are set in the Trunk/LACP Interface are identically set in all member ports, and cannot be set in each member port directly.
ALL	Is used to apply the same configuration to all ports.
TGID	Indicates the TGID in which the port is involved, if the port is a member of the Trunk/LACP.
Active	Sets whether to make the port active or not
Auto Negotiation	Specifies Auto Negotiation. [Auto] activates Auto Negotiation and [Forced] inactivates Auto Negotiation.
Jumbo	Is used for activation/inactivation of Jumbo Frame setup. The activated port allows the forwarding for the frame up to 9,216 Bytes.
Flow Ctrl	Sets whether to perform the Flow Control, and is divided into Tx and Rx.

Categories	Description
Storm Ctrl	Sets whether to perform the Storm Control, and is divided into Bcast (Broadcast), Mcast (Multicast), and DLF (Destination Lookup Failure).

Statistics

Select **[Port]** → **[Statistics]** menu to display the statistic information of a port.
Press the **[Refresh]** button to update the displayed information. Press the **[Reset]** button to reset all statistics to '0'.

Statistics

The Statistics window displays the statistic information on each port.

Statistics								
Port	Link	Input Packets	Input Dropped	Input Errors	Output Packets	Output Dropped	Output Errors	Collisions
Port1	Off	0	0	0	3	0	0	0
Port2	Off	0	0	0	3	0	0	0
Port3	Off	0	0	0	3	0	0	0
Port4	Off	0	0	0	3	0	0	0
Port5	Off	0	0	0	3	0	0	0
Port6	Off	1990	1456	0	602	0	0	0
Port7	Off	783	27	0	884	0	0	0
Port8	Off	0	0	0	3	0	0	0
Port9	On	1114	553	0	617	0	0	0
Port10	Off	0	0	0	3	0	0	0

Categories	Description
Port	Displays ports.
Link	Displays the status of link up/down.
Input Packets	Displays the number of the Input Packets until now.
Input Dropped	Displays the current Input Dropped numbers.
Input Errors	Displays the number of the Input Errors until now.
Output Packets	Displays the number of the Output* Packets until now.
Output Dropped	Displays the currently output dropped numbers.
Output Errors	Displays the number of the Output Error until now.
Collisions	Displays the number of the Collision until now.

Mirror Config.

Select **[Port]** → **[Mirror Config]** menu to perform the port mirroring.

To apply the configurations specified, press the **[OK]** button. To cancel the newly configured data, press the **[Cancel]** button.

Mirroring Configuration

Only one “Mirror-To Port” can be specified and the Mirror-To Port and the Mirrored Port cannot be the same. Ingress for the packets received(Rx) and Egress for the packets transmitted (Tx) in the corresponding port can be monitored in the Mirror-To Port. Both configurations contain Rx and Tx.

Port	1	2	3	4	5	6	7	8	9	10
Mirror-To Port	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Mirrored Port	N ▼	N ▼	N ▼	N ▼	N ▼	N ▼	N ▼	N ▼	N ▼	N ▼
Option	(N: None, B: Both, I: Ingress, E: Egress)									

OK Cancel

Categories	Description
Port	Displays the port number.
Mirror-To Port	Configures Mirror-To Port.
Mirrored Port	Configures Mirror-To Port.
Option	Describes each option symbol.

Forward Table

[Port] → Select the **[Forward Table]** menu to see the learned MAC address of each port. Press the **[Refresh]** button to update the displayed information.

The Forward Table window displays the MAC address information discovered for each port.

Port	Vlan	MAC	MAC Type	Learn Type
Port6	1	0000.f04d.0b06	Unicast	Static
Port9	1	0000.f0a1.23a7	Unicast	Dynamic
Port9	1	0013.2032.0994	Unicast	Dynamic
Port9	1	0009.7400.1003	Unicast	Dynamic
Port9	1	000c.f1cf.e604	Unicast	Dynamic
Port9	1	0013.801e.2a80	Unicast	Dynamic
Port9	1	0000.f0da.debb	Unicast	Dynamic
Port9	1	0007.e9ef.b4fd	Unicast	Dynamic
Port9	1	0001.02fd.4684	Unicast	Dynamic
Port9	1	0002.3f6b.bc43	Unicast	Dynamic
Port9	1	a000.ff00.072a	Unicast	Dynamic

Reset

Categories	Description
Port	Displays ports.
VLAN	Displays VLAN pertaining to the port.
MAC	Displays the MAC Address learned.
MAC Type	Displays the type of MAC address.
Learn Type	Displays the Learn type of MAC address.

VLAN

Configuration

[VLAN] → [Configuration]

To apply the specified configuration, press the **[Save]** button.

To initialize the configuration, press the **[Reset]** button.

Port Setup

The Port Setup window is used for the configuration of the VLAN ID for each port or Ingress Filter for VLAN Security. The type of packets coming from the port can be limited via the Frame-Type. If the port is selected as Tagged-packet and Untagged-packet is flown in, the packet is discarded.

Port Setup

Port ID	PVID	Ingress-filter	Frame-type
1	1	Disable	All-Packet

Save
Reset

Categories	Description
Port ID	Displays the port to be configured.
PVID	Specifies the default VLAN IN of a port. The ID can be selected from the currently configured VLAN.
Ingress-Filter	Determines the use of Ingress Filtering (Enable/Disable).
Frame Type	Configures Ingress Packet. (All-Packet/Tagged-Packet).

VLAN Create

Enter the VLAN ID and then press the **[Save]** button to create a new VLAN.

VLAN Create

VLAN Create	
VLAN-ID	(2 - 4094)

Save
Reset

VLAN Edit

The VLAN window is used for the addition or deletion of members to/from the created VLAN. If Egress-Tagged is selected, the packet that sends out to the outside via a port is sent out as Tagged-Packet. To delete the created VLAN, press the **[Delete]** button. At this time, all member ports pertaining to VLAN are deleted.

VLAN Edit

Parameter	Argument
VLAN-ID	100
VLAN Name	VLAN0100
VLAN Member	1 2 3 4 5 6 7 8 9 10 ☒ ☒ ☒ ☒ ☐ ☐ ☐ ☐ ☐ ☐
Egress-Tagged	1 2 3 4 5 6 7 8 9 10 ☒ ☐ ☒ ☐ ☐ ☐ ☐ ☐ ☐ ☐

If the port is set as the trunk port (Static Trunk), the port is hidden and the trunk device is displayed. The member port of each group should have always the same VLAN characteristics. Therefore, the ports with the different VLAN characteristics cannot be involved in the trunk group. In case of LACP, if the link of its member port is not connected, the trunk device is hidden.

The trunk device is displayed like sa1, sa2, ... in case of Static Trunk, and displayed like Po1, Po2, ... in case of LACP.

Categories	Description
VLAN-ID	Displays the VLAN-ID to be configured.
VLAN Name	Configures a name to VLAN.
VLAN Member	Selects members to VLAN.
Egress-Tagged	Selects the type of the Egress packet.(as Tagged or Untagged).

VLAN Classification

VLAN Classification is used to set parameter according to classification of VALN. If, among the data configured by a user, an overlapped data exists among MAC-Based, IP-Based and Protocol-Based configurations, the MAC-based configuration has the highest priority. If the MAC-based configuration does not exist, the IP-based configuration has the next highest priority. The protocol-based configuration has the lowest priority.

Categories	Description
Classification Mode	Selects the type of VLAN classification.
Group ID	Specifies the group ID to be configured.
VLAN ID	Specifies the VLAN ID to be configured. The ID can be selected from the created VLANs.

Categories	Description
Classification Rule	Differently displays the window to select the rule in accordance with VLAN Classification.

MAC based VLAN

If MAC is selected in classification mode, the VLAN Configuration window is displayed. This window is used for the configuration of VLAN in accordance with the source MAC address of the Untagged packet arriving to the port.

VLAN Classification

Parameter	Argument
Classification Mode	MAC
VLAN ID	2
Group ID	1 (1-1024)
Classification Rule	00 : 0f : 00 : 12 : 00 : 11

Save Reset

IP Based VLAN

If IP-subnet is selected in classification mode, the following configuration window is displayed. This window is used to configure VLAN depending on the IP subnet of the Untagged packet coming in the port.

VLAN Classification

Parameter	Argument
Classification Mode	IP-Subnet
VLAN ID	2
Group ID	1025 (1025-1153)
Classification Rule	192 . 168 . 0 . 0 / 24

Save Reset

Protocol Based VLAN

If Protocol is selected in classification mode, the following configuration window is displayed. This window is used to configure VLAN depending on the protocol type of the Untagged packet coming in the corresponding port selected in the following figure: In the Classification Rule, a protocol can be selected and a user can enter the protocol number as hexadecimal value. If the port is set as the trunk group, the same setting is to be made in all member ports of the trunk group.

VLAN Classification

Parameter	Argument
Classification Mode	Protocol
VLAN ID	2
Group ID	1154 (1154-1314)
Classification Rule	IP (Hex)
Port Num	port1 (Only Protocol VLAN)

Save Reset

Status

[VLAN] → [Status] menu displays the information on the currently configured VLAN.

VLAN Information

The VLAN Information window displays the configuration of the Ingress-Filter and the Acceptable Frame-Type for each port.

VLAN Information			
Port ID	PVID	Ingress-filter	Frame-type
Port1	100	Disable	All-Packet
Port2	100	Disable	All-Packet
Port3	100	Disable	All-Packet
Port4	100	Disable	All-Packet
Port5	1	Disable	All-Packet
Port6	1	Disable	All-Packet
Port7	200	Disable	All-Packet
Port8	200	Disable	All-Packet
Port9	200	Disable	All-Packet
Port10	200	Disable	All-Packet

The VLAN Information window displays the information on the VLAN configuration.

VLAN Information												
ID	VLAN Information											
1	default	Member Ports	1	2	3	4	5	6	7	8	9	10
		Egress Tagged	☐	☐	☐	☐	☒	☒	☐	☐	☐	☐
100	VLAN0100	Member Ports	☒	☒	☒	☒	☐	☐	☐	☐	☐	☐
		Egress Tagged	☒	☒	☐	☐	☐	☐	☐	☐	☐	☐
200	VLAN0200	Member Ports	☐	☐	☐	☐	☐	☐	☒	☒	☒	☒
		Egress Tagged	☐	☐	☐	☐	☐	☐	☒	☒	☐	☐

VLAN Classification Information

The VLAN Information window displays the information on the VLAN configuration.

To cancel the configuration, select the configuration to cancel and press the **[Delete]** button. In case of the protocol classification, the trunk member cannot be removed separately. Use the **[Refresh]** to view the latest information.

VLAN Classification Information					
☐	Group ID	MODE	VID	Classifier	Port
☐	1	MAC	2	0f.012.011	
☐	1025	IP-Subnet	2	192.168.0.0/24	
☐	1154	Protocol	2	ip	sa1
☒	1155	Protocol	2	ip	port1
☐	1156	Protocol	2	ip	port2

Layer2 Menu

Select the **[Layer2]** menu. The submenus will be displayed in the upper left side of the window as follows:

Layer2	
▢ RSTP	
▶ Configuration	Status
▢ Port Trunking	
Configuration	Status
▢ GVRP	
Configuration	Status
▢ IGMP Snooping	
Time Interval	Function
Multicast Filter	Forwarding Table
Management	
▢ Authentication	
Configuration	Management

Menu	Sub-menu	Description
RSTP	Configuration	Prevents broadcast storms caused by switch loop-backs.
	Status	Display the configuration for RSTP.
Port Trunking	Configuration	Specifies the setup related to Static Trunk or LACP by using Port Trunking.
	Status	Display the information on the Static Trunk and the LACP configurations.
GVRP	Configuration	Enables GVRP. Enables the virtual VLAN control by using GVRP.
	Status	Displays the information configured in [VLAN] → [Configuration] menu.
IGMP	Time Interval	Sets the time related to IGMP Snooping.
	Function	Sets the functions related to IGMP Snooping.
	Multicast Filter	Defines the operation type for Multicast Packet.
	Forwarding Table	Displays the information on the members registered in IGMP Group.

Menu	Sub-menu	Description
	Management	Activates/inactivates the operation of IGMP Snooping.
Authentication	Configuration	Sets the Authentication for each port.
	Management	Performs the configuration for the Authentication and the RADIUS Server.

RSTP

The **[RSTP]** configuration menu configures loop detection from several switches or a single switch link.

Configuration

Select **[RSTP] → [Configuration]** menu to configure the Bridge or Port environment to be used in the RSTP protocol.

Protocol Status

Parameter	Argument
RSTP status	Current Enable

Bridge Parameter

Parameter	Argument
Bridge Priority	8 Default : 8 (0 - 15)
Hello Time	2 sec Default : 2 (1 - 10)
Max Age Time	20 sec Default : 20 (6 - 40)
Forward Time	15 sec Default : 15 (4 - 30)

Port Parameter

Port Name	Priority	Force Version	Path Cost	Port Fast	Link Type
Port 1	8	RSTP	20000	Enable	Shared
Port 2	8	RSTP	20000	Enable	Shared
Port 3	8	RSTP	20000	Enable	Shared
Port 4	8	RSTP	20000	Enable	Shared
Port 5	8	RSTP	20000	Enable	Shared
Port 6	8	RSTP	20000	Enable	Shared
Port 7	8	RSTP	20000	Enable	Shared
Port 8	8	RSTP	20000	Enable	Shared
Port 9	8	RSTP	20000	Enable	Shared
Port 10	8	RSTP	20000	Enable	Shared

Save
Reset

Categories	Description
Protocol Status	Displays the current status of the RSTP protocol.
Bridge Parameter	- Bridge Priority: Sets the priority of Bridges. - Hello Time: Sets the transmission cycle of BPDU. - Max Age Time: Sets the Message Age time. - Forward Time: Displays the time that the state of each port is changed by level.(Discarding-Learning-Forwarding)
Port Parameter	- Priority: Standard to select the port to be blocked when the switch loop is established. - Force Version: Communication is transmitted via the switch connected to the corresponding port and the BPDU that a user specifies. For '0', STP BPDU is transmitted. For '1', RSTP BPDU is transmitted. - Path Cost: Displays the path cost according to the bandwidth when a connection is established. - Port Fast: If this value is activated, the corresponding port becomes an Edge port and is quickly converted into a forwarding state by considering the port is connected to a terminal device, not a switch device. In addition, if this function is activated, the MAC address learned in the corresponding port is not cancelled even when all topologies of Bridges are changed. (To connect the port to the STP device, the Port Fast function should be cancelled.) - Link Type: Displays the type of the link connected to the opponent. The link is connected as point-to-point in RSTP.

Status

[RSTP] → [Status] menu is used to display the status of switch RSTP operation. The status is roughly divided into Bridge Information and Port Information.

The Bridge Information Category in the upper section displays the RSTP parameter configured in the system and the Port Information item in the lower section displays the detailed information by ports.

Bridge Information					
Parameter	Argument				
Protocol Status	Enabled				
Designated Bridge Identifier	80000000f0e80131				
Root Bridge Identifier	80000000f0444444				
Root Path Cost	20000				
Root Port	12				
Last Topology changed	Sun Jan 22 18:03:16 2006				

Port Information					
Port Name	Port ID	Path Cost	Port Role	Port State	Designated Root
Port1	0x8003	20000	Disabled	Discarding	00000000f0e80131
Port2	0x8004	20000	Disabled	Discarding	0000000000000000
Port3	0x8005	20000	Disabled	Discarding	0000000000000000
Port4	0x8006	20000	Disabled	Discarding	0000000000000000
Port5	0x8007	20000	Disabled	Discarding	0000000000000000
Port6	0x8008	20000	Disabled	Discarding	0000000000000000
Port7	0x8009	20000	Disabled	Discarding	0000000000000000
Port8	0x800a	20000	Disabled	Discarding	0000000000000000
Port9	0x800b	20000	Disabled	Discarding	0000000000000000
Port10	0x800c	20000	Rootport	Forwarding	80000000f0444444

[Refresh](#)

Bridge Information

- **Designed Bridge Identifier**
Its own bridge information is displayed in hexadecimal numbers. The upper four digits represent the bridge priority and the remaining lower digits are expressed as the system MAC address.
- **Root Bridge Identifier**
Among the connected switches, it indicates the identifier of the switch equipment selected as the root bridge. Therefore, if there is no connection between switches, the Root Bridge Identifier displays the same information as the Designed Bridge Identifier.
- **Root Path Cost**
When the root bridge is connected it displays the calculated cost for the path to the root switch.
- **Root Port**
If the current equipment is not designated as the root switch, this field indicates the ID of the port corresponding to the root port.

- **Last Topology Changed**
It indicates the recent time that the RSTP network is reconfigured by the change of the network configuration between switches.

Port Information

- **Port ID**
The value is combined with the value of the port priority and the ID value of the port specified in the system. The highest two digits represents the value of the port priority and the lowest two digits consist of port index.
- **Path Cost**
The value indicates the path cost of the corresponding path.
- **Port Role**
The value indicates the role of the port that selected via the BDPU exchange between switches. The RSTP Port Role is divided into Disable, Alternate, Backup, Designated, Root roles.
- **Port State**
The port state shows the status of the corresponding port. If a loop is detected via the BDPU communication, the Port State looks for the port to be blocked in accordance with Port ID and Path Cost and blocks data communication to prevent the loop from being constructed in the whole switch. The port state is divided into Discarding, Learning, Forwarding and Blocking states. In blocking, learning, discarding states, data communication is not performed. The data communication is performed only in forwarding state. In addition, the blocking state represents the state that blocks the data communication by force by detecting a loop via RSTP.
- **Designated Root**
If a switch connected to the corresponding port is closer to the root switch, the Designated Root shows the Bridge identifier of the connected switch. Otherwise, the designated Root shows its own Bridge identifier.

Port Trunking

Configuration

Select the **[Port Trunking] → [Configuration]** menu to specify the configuration related to Port Trunking. To apply the configurations, press the **[Save]** button. To default the configuration, press the **[Reset]** button.

LACP Configuration

The LACP Configuration window can configure trunk groups and add or delete members.

LACP Configuration

Parameter	Argument
Group ID	1 ▾
Group Mode	Trunk ▾
Group Member	12345678910 ☐☐☐☐☐☐☐☐☐☐

[Edit](#)

Categories	Description
Group ID	Selects a group number from 1 to 8.
Group Mode	[Trunk] indicates the use of Static Trunking, and [LACP] indicates the use of LACP protocol. LACP is distinguished with Static Trunking in that the configuration as the LACP port automatically forms bandwidth.
Group Member	Selects the members of a group. Up to eight members can be specified.
LACP Mode	Appears when [LACP] is selected in Group mode. In LACP mode, [Active/Passive] can be selected. In Active mode, if a port is connected with a link, the standard system sends LACP packets to the opposite system first. In passive mode, the relevant port replies only when the port receives a packet from the opposite system. If both of the user system and the opposite system are set to Active, the system with higher priority becomes the standard system.

Load Balance

When packets are sent to the opposite system via a trunk port, the packets are transmitted to the port of members pertaining to the trunk group. The Load Balance window is used for the selection of the algorithm to select the port to sent out the packets.

Load Balance

Group ID	Load Balance Mode
1	Source + Destination MAC Address

Categories	Description
Group ID	Selects a group number among 1 to 8.
Load Balance Mode	A total of six algorithms are provided. The default value is Source MAC Address + Destination MAC Address. - Source MAC Address - Destination MAC Address - Source MAC Address + Destination MAC Address - Source IP Address - Destination IP Address - Source IP Address + Destination IP Address

LACP Priority

The LACP Priority window is used for the configuration of the system priority and the port priority. Only LACP ports can be configured.

LACP Priority

VLAN ID	NAME	
System Priority		(1 - 65535 Default : 32768)
Port Priority	1	(1 - 65535 Default : 32768)

Categories	Description
System Priority	Displays the priority of the system. The default value is 32768.
Port Priority	Configures the priority of ports. The default value is 32768.

Status

Select **[Port Trunking] → [Status]** menu to specify the configuration related to Port Trunking.

Use the **[Refresh]** button to update the information.

System Priority

The System Priority window shows the system priority information and the system ID.

System Priority	
System Priority	System ID
8000	00-00-f0-00-00-00

Trunking

The Trunking window shows the Static Trunk information configured in the system.

Trunking											
Group ID	Load Balance Mode	Group Members									
1	SRC+DST MAC	1	2	3	4	5	6	7	8	9	10
		☒	☒	☒	☐	☐	☐	☐	☐	☐	☐

LACP

The LACP window displays the LACP information configured in the system.

LACP				
Port	Group ID	Group Mode	Load Balance Mode	Priority
Port8	2	Active	SRC+DST MAC	0x8000
Port9	2	Passive	SRC+DST MAC	0x8000
Port10	2	Active	SRC+DST MAC	0x8000

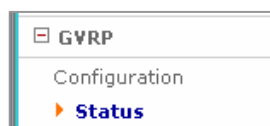
LACP Port Sync

The LACP Port Sync window displays the information on the ports connected to the opposite system among ports composed with LACP ports. If the LACP group is configured in the **[Configuration]** menu but the port is not connected to the opposite system, the LACP information may not be displayed. Ports marked with 'O' in the Sync Category are ports that normally operate as LACP ports.

LACP Port Sync		
Group ID	Member Port	Sync
2	Port8	O
	Port9	O
	Port10	O
Refresh		

GVRP

Select the **[Layer2]** menu. The submenus will be displayed in the upper left side of the window as follows:



Menu	Submenu	Description
GVRP	Configuration	Configures GVRP.
	Status	Displays the configuration status of GVRP.

The **[GVRP]** menu is used to start/stop the GVRP service or change the information on the GVRP service status of each port.

Configuration

Select the **[GVRP] → [Configuration]** menu to start/stop the GVRP and the Dynamic VLAN Creation services.

GVRP Basic	
Parameter	Argument
GVRP	Enable ▼
Dynamic Vlan Creation	Enable ▼
Save	

The description of the menu button is as follows:

Categories	Description
Save	Save the configurations for GVRP and Dynamic VLAN Creation.

On the <GVRP Basic> window, enable the GVRP configuration and click the **[Save]** button to display the following window.

GVRP Configuration

Port	Status	Registration	Applicant	Timers(millisecond)		
				Join	Leave	LeaveAll
☐ ALL	Enable	-	-	-	-	-
port1	Disable	-	-	-	-	-
port2	Disable	-	-	-	-	-
port3	Disable	-	-	-	-	-
port4	Disable	-	-	-	-	-
port7	Disable	-	-	-	-	-
port8	Disable	-	-	-	-	-
port9	Disable	-	-	-	-	-
port10	Disable	-	-	-	-	-

OK
Refresh

Categories	Description
Port	Port Number
Status	GVRP configuration Information
Registration	Registration mode with Normal, Forbidden and Fixed conditions
Applicant	Applicant mode with Normal and Active conditions
Join	Interval for Join Transfer Time
Leave	Value of Leave Delay Time
LeaveAll	Value of LeaveAll Transfer Time

The description of the menu buttons are listed in the table below.

Categories	Description
OK	Stores the information of the modified ports.
Refresh	Displays the latest information of ports.

Status

Select **[GVRP] → [Status]** to display the GVRP configuration.

GVRP Machine

Port	Applicant State	Registrar State
Port1	VO	MT
Port2	VO	MT

GVRP statistics

Port		Join Empty	Join In	Leave Empty	Leave In	Empty
Port1	RX	0	0	0	0	0
	TX	0	0	0	0	0
Port2	RX	0	0	0	0	0
	TX	0	0	0	0	0

Refresh

GVRP Machine

Categories	Description
Port	Port Number
Applicant State	Current Status of Applicant State Machine
Register State	Current Status of Register State Machine

GVRP Statistics

Categories	Description
Port	Port Number
Join Empty	Number of Join Empty packets
Join In	Number of Join In packets
Leave Empty	Number of Leave Empty packets
Leave In	Number of Leave In packets
Empty	Number of Empty packets

The description of the menu buttons are listed in the table below.

Categories	Description
Refresh	Displays the latest information of the port that GVRP is configured.

IGMP Snooping

The **[IGMP Snooping]** menu is used to configure IGMP Snooping.

Time Interval

Select the **[IGMP Snooping] → [Time Interval]** menu to configure the time related to IGMP Snooping.

Time Interval

Category	Argument
VLAN	Default
Group Membership	120000 ms

OK

VLAN	Group Membership (ms)	Last Member Query (ms)	Max Response (ms)	Other Query (ms)
Default	120000	1000	10000	120000

Categories	Description
VLAN	Selects the VLAN to be configured.
Group Membership	Configures the time to exit from the multicast forwarding database list when new report does not exist.
Last Member Query	Indicates the time to wait for a response report after sending a query to check if the host is the last host when multicast router receives a leave message from a host. If the report is not replied until the time is elapsed, the host is deleted from the group.
Max Response	Configures the maximum time until its response when IGMP Snooping query is received.
Other Query	Configures the time until the operation as a querier starts when a query from the multicast router does not exist.

Select the VLAN and the Category to configure, enter the time and click the **[OK]** button to store the configuration.

Function

Select **[IGMP Snooping]** → **[Function]** menu to specify the functions related to IGMP Snooping.

Function

Category	Argument
VLAN	Default
Querier	Disable

OK

VLAN	Querier	Immediate Leave
Default	Disable	Disable

Categories	Description
VLAN	Selects the VLAN to be configured.
Querier	Specifies the operation as IGMP querier when the multicast router does not exist.
Immediate Leave	Deletes a host from the group immediately when receiving the Leave Message.

Multicast Filter

Select **[IGMP Snooping]** → **[Multicast Filter]** menu to specify the functions related to IGMP Snooping.

Multicast Filter

Category	Argument
Port 1	Forward group
Port 2	Forward group
Port 3	Forward group
Port 4	Forward group
Port 5	Forward group
Port 6	Forward group
Port 7	Forward group
Port 8	Forward group
Port 9	Forward group
Port 10	Forward group

OK

Categories	Description
Forward Group	Always forwards multicast packets.

Categories	Description
Filter unregistered group	Drops multicast packets when any member pertaining to IGMP group does not exist.
Forward unregistered group	Forwards multicast packets when any member pertaining to IGMP group does not exist.

Forwarding Table

Select **[IGMP Snooping] → [Forwarding Table]** menu to display the information on the members registered in IGMP Group.

Forwarding Table

VLAN	Multicast IP Address	Member Port	Aging Time
------	----------------------	-------------	------------

Refresh

Click the **[Refresh]** button to update the information displayed on the web screen into the latest information.

Management

Select **[IGMP Snooping] → [Management]** menu to specify the operation of IGMP Snooping.

If Global is set to Disable, all VLANs will be disabled.

IGMP Snooping Management

Scope	Action
Global	Enable

OK

Scope	Current Status
Global	Enable
Default	Enable



NOTE

IGMP Snooping Management

In the Global Disabled mode, other pages with the exception of the the Management page will not be displayed.

Authentication

This menu is used to set/retrieve authentication information.

Configuration

When selecting **[Authentication] → [Configuration]** if the activity status of **[Authentication] → [Management]** is 'Stop', the following window appears:

Authentication Configuration

802.1X Port-Based Authentication Disabled

If **[Authentication] → [Management]** is 'Running', the following window will appear:

Authentication Configuration

Port	Control	Reauth	Reauth-period	Tx-period	Supp Time-out	Server Time-out
Port1	None	☐				
Port2	None	☐				
Port3	None	☐				
Port4	Auto	☐	3600	30	30	30
Port5	None	☐				
Port6	None	☐				
Port7	None	☐				
Port8	None	☐				
Port9	None	☐				
Port10	None	☐				

Item	Description
Control	Indicates the authentication mode for each port. - None: Authentication is not performed for the port. - Force-authorized: Admits the port forcibly. - Force-unauthorized: Block the port forcibly. - Auto: Allows the port through authentication from the Radius server and blocks the port.
Reauth	Used for re-authentication.
Reauth-Period	Indicates re-authentication cycle when Reauth is set. (1-4294967295sec) default: 3600sec
Tx-Period	Indicates the cycle that sends Request regularly to supplicant.(1-65535sec) default: 30sec

Item	Description
Supp-Timeout	Indicates the time before re-sending to the user when EAP is requested. (1-65535sec) default: 30sec
Sever-Timeout	Indicates the time before re-sending to the device when server authentication of a server is requested. (1-65535sec) default: 30sec

When authentication is forcibly performed for the port in Control mode, select Force-authorized. When authentication is not forcibly performed, select Force-unauthorized. Set to Auto to be authenticated from Radius. Click the **[OK]** button to apply the authentication.

Management

Select **[Authentication]** → **[Management]** to activate/deactivate authentication of the system.

Setting 802.1x user authentication indicates that there is the Radius server that has the user information. The host IP address, host, and key should be registered of the Radius server to be used. The default of the Radius Host Port is 1812 port.

Click the **[OK]** button after the setting. Then, the setting is applied.

Authentication Management

Activity	Action
Stop	Run

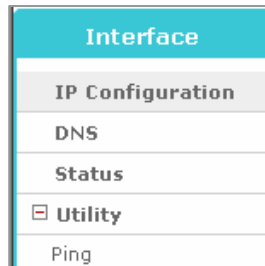
Radius Server Management

Host IP	192 . 168 . 0 . 23
Secret Key	samsung
Host Port	1812

OK
Cancel

Interface

Select the **[Interface]** menu. The submenus will be displayed in the upper left side of the window as follows:



Menu	Submenu	Description
IP Configuration	-	Sets an IP address of a VLAN device.
DNS	-	Sets a name server used in GSIM.
Status	-	Displays the IP address or MAC information currently being set in a VLAN device.
Utility	Ping	Checks the network by executing the ping.

IP Configuration

This menu is used to set an IP and Administrative up/down.

Network Interface

Select a VLAN device to set the corresponding IP address and Netmask or to set whether to use an interface. Select the target item and click the **[OK]** button.

 A screenshot of a "Network Interface" configuration window. At the top, there's a section titled "Rd Interface" with a dropdown menu showing "rd1". Below this is a section titled "Interface" containing three rows: "IP" with input fields for 10, 0, 3, and 1; "Netmask" with input fields for 255, 255, 255, and 0; and "Interface Up" with radio buttons for "On" (selected) and "Off".

Menu	Submenu	Description
Rd Interface	-	Sets a VLAN device that exists in GSIM.
IP	-	Sets a Network IP.
Netmask	-	Sets a Netmask.
Interface Up	-	Sets whether to activate/deactivate.

IP Alias

This menu is used to allocate an additional IP address to the corresponding interface.

IP Alias

	IP	Netmask
☐	100 . 0 . 0 . 1	255 . 255 . 255 . 0

Add
Delete

DNS

This menu is used to set the name server used by the GSIM.

Name Server Add

168 . 126 . 63 . 1

Add

Set the IP corresponding to the DNS server and click the **[Add]** button.

The setting is directly applied to the <Static DNS> of **[Interface] → [DNS]**. For example, when DNS is entered, the <Static DNS> window is displayed as follows:

Static DNS

Name Server List	
☐	168.126.63.1

Delete

Status

This menu is used to retrieve the Interface information from the GSIM.

Menu	Submenu	Description
Interface	-	Interface name
IP	-	IP address information
Netmask	-	Netmask information
Status	-	Whether to activate/deactivate

Network Status

Interface	IP	Netmask	Status	MAC Address
rd1	10.0.3.1	255.255.255.0	up	0000.f000.0000
rd100	1.1.1.1	255.255.255.0	down	0000.f000.0000

Utility

Select the **[Interface]** menu. The submenus will be displayed in the upper left side of the window as follows:

Interface
IP Configuration
DNS
Status
☒ Utility
Ping

Ping inspects whether the IP datagram reaches other host by using the application program that uses the TCP/IP protocol. The program using the ping sends the message of the ICMP echo request to the remote host, and waits the response. If the host that has received the transferred ICMP echo request is in use, the response is made. If no operation, the response is not made. Like this, whether the operation of the remote host can be verified with the return of the ICMP echo reply.

Ping

This page sets and executes the ping test. When this item is selected, the following screen is displayed. The details on each item are as follows:

Ping

Destination IP	Action
☒ . . .	Run
☐ . . .	
☐ . . .	

In the **[Destination IP]**, enter the destination address of the remote host to confirm the connection. Click the [Run] button, then the ping test starts.

Only one destination IP can be tested at a time.

Ping

Destination IP	Action
☒ 192 . 168 . 0 . 1	Run
☐	
☐	

Log

```
PING 192.168.0.1 (192.168.0.1) from 192.168.18.100 : 56(84) bytes of data.  
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=0.279 ms  
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=0.129 ms  
64 bytes from 192.168.0.1: icmp_seq=3 ttl=64 time=0.129 ms  
--- 192.168.0.1 ping statistics ---  
3 packets transmitted, 3 received, 0% loss, time 1998ms  
rtt min/avg/max/mdev = 0.129/0.179/0.279/0.070 ms
```

Layer 3 Menu

Select the **[Layer3]** menu. The submenus will be displayed in the upper left side of the window as follows:

Layer3	
General	
Routes	
Management	
Configuration	
Static	
RIP	
RIP Interface	
OSPF	
OSPF Interface	
BGP	
List	
Access List	
Prefix List	
Route Map	
AS path List	
Community List	
Key Chain	
Status	
RIP	
OSPF	
BGP	

Menu	Submenu	Description
General	Routes	Displays the routing table of GSIM.
	Management	Starts or stops RIP, OSPF, and BGP.
Configuration	Static	Sets a static route.
	RIP	Sets RIP.
	RIP Interface	Sets RIP interface.
	OSPF	Sets OSPF protocol.
	OSPF Interface	Sets OSPF interface.
	BGP	Sets BGP.
List	Access List	Sets Access-list.
	Prefix List	Sets Prefix-list.
	Route Map	Sets Route-map.
	AS-Path List	Sets BGP AS-path list.
	Community List	Sets BGP Community-list.
	Key Chain	Sets the key used for authentication of RIP v2.

Menu	Submenu	Description
Status	RIP	Displays RIP network information.
	OSPF	Displays OSPF neighbor information.
	BGP	Displays the Neighbor status connected with the BGP network information.

General

This menu is used to start/stop RIP, OSPF, and BGP services or to retrieve routing table information.

Routes

Select **[General]** → **[Routes]** to retrieve routing table information.

Routes		
Type	Network	Entry
S	100.0.0.0/24	[1/0] via 10.0.3.100 inactive
C *>	127.0.0.0/8	is directly connected, lo
C *>	192.168.0.0/24	is directly connected, eth0

Refresh

Menu	Submenu	Description
Type	-	- C: Network directly connected to GSIM network interface - S: Static network set by a user - R: Path information received from another router via RIP - O: Path information received from another router via OSPF protocol - B: Path information received from another router via BGP - *>: Whether to have activated routing table
Network	-	Network/Netmask information of route
Entry	-	Route information

Management

Select **[General]** → **[Management]** to start/stop RIP, OSPF, and BGP services.

Management		
Protocol	Current Status	Action
RIP	Start	On
OSPF	Start	On
BGP	Start	On

OK

Configuration

This menu is used to set static routes, RIP, OSPF protocol, and BGP.

Static Route

Select **[Configuration] → [Static]** and set a static route. After setting the target item, click the **[Save]** button.

Static

Enter the Static Route setting command.

Static

Command

OK

Routes

Type	Network	Entry
S	100.0.0.0/24	[1/0] via 10.0.3.100 inactive
C *>	127.0.0.0/8	is directly connected, lo
C *>	192.168.0.0/24	is directly connected, eth0

Refresh

When the entered command is successfully executed, the setting is directly applied to **<Current Status>** of **[Layer3] → [Configuration] → [Static]**.

For example, when entering the static route command, the **<Current Status>** window is displayed as follows:

Help

Select the argument corresponding to the 'ip route' or 'no ip route' command. Click **[Argument]** to display all arguments corresponding to the command. Select an argument from them.

Help

Command	Argument
ip route	A.B.C.D A.B.C.D (A.B.C.D)INTERFACE

Current Status

Displays the static table from the routing tables of the GSIM.

Current Status		
Type	Network	Entry
S *>	0.0.0.0/0	[1/0] via 192.168.0.1, eth0
S *>	200.0.1.0/24	[1/0] via 192.168.18.200, eth0

Menu	Submenu	Description
Type	-	- S: Static network ser by a user - *>: Whether to include activated routing table
Network	-	Network/Netmask information of route
Entry	-	Route information

RIP

Select **[Configuration]** → **[RIP]** and set RIP. Enter the RIP command.

RIP

Command

OK

If the entered command is successfully executed, the execution result is directly applied to <Current Status> of **[Router]** → **[Configuration]** → **[RIP]**.

Help

Select the argument corresponding to the RIP command. Clicking the **[Argument]** item displays all information corresponding to the command.

Help

Command	Argument
default-information	originate

RIP Basic

After selecting each item, click the **[OK]** button. Then, the applied value is displayed in the **<Current Status>** window.

RIP Basic

Command	Argument
Version	☐ 1 ☒ 2 (default)
redistribute	☐ connected ☐ static ☐ ospf ☐ bgp
network	. . . /

OK

Current Status

Displays the command setting currently entered.

Current Status

Router RIP
No Entry

Delete

RIP Interface

Select **[Configuration] → [RIP Interface]** and set RIP. Select the target interface and enter the protocol setting command directly.

RIP Interface

Interface	Command
rd1	

OK

If the entered command is successfully executed, the execution result is directly applied to **<Current Status>** of **[Router] → [Configuration] → [RIP Interface]**.

Help

Select the argument corresponding to the RIP interface.

Clicking the **[Argument]** item displays all arguments corresponding to the command. Select an argument from them.

Help

Command	Argument
ip rip	authentication key-chain LINE

RIP Interface Basic

After selecting each item, click the **[OK]** button. Then, the applied value is displayed in the **<Current Status>** window.

RIP Interface Basic

Command	Argument
receive version	☐ 1 ☐ 2
send version	☐ 1 ☐ 2

OK

Current Status

Displays the command setting currently entered.

Current Status

Router RIP Interface rd1

No Entry

OSPF

[Configuration] → [OSPF]

OSPF

Command

OK

If the entered command is successfully executed, the execution result is directly applied to <Current Status> of [Router] → [Configuration] → [OSPF].

Help

Select the argument corresponding to the OSPF command.

Help

Command	Argument
area	{A.B.C.D <0-4294967295>} authentication

OSPF Basic

After selecting each item, click the [OK] button. .

OSPF Basic

Command	Argument
redistribute	☐ connected ☐ static ☐ rip ☐ bgp
network	. . . / area ID

OK

Current Status

Displays the command setting currently entered.

Current Status

Router OSPF

No Entry

Delete

OSPF Interface

Select **[Configuration]** → **[OSPF Interface]** to set OSPF protocol. Select the target interface and enter the protocol setting command directly.

OSPF Interface

Interface	Command
rd1	

OK

If the entered command is successfully executed, the execution result is directly applied to **<Current Status>** of **[Router]** → **[Configuration]** → **[OSPF Interface]**.

Help

Clicking the **[Argument]** item displays all arguments corresponding to the command.

Help

Command	Argument
ip ospf	A.B.C.D authentication (null message-digest)

OSPF Interface Basic

OSPF Interface Basic

Command	Argument
cost	<1-65535> Cost
dead-interval	<1-65535> Seconds
hello-interval	<1-65535> Seconds
transmit-delay	<1-65535> Seconds
retransmit-interval	<1-65535> Seconds

OK

Current Status

Displays the command setting currently entered.

Current Status

Router OSPF Interface rd1
No Entry

BGP

Select **[Configuration]** → **[BGP]** and set BGP. After setting the target item the **[Save]** button. Enter the BGP setting command directly.

BGP

Command
network 100.0.0.0/24

OK

If the entered command is successfully executed, the execution result is directly applied to **<Current Status>** of **[Layer3]** → **[Configuration]** → **[BGP]**.

Help

Clicking the **[Argument]** item displays all arguments corresponding to the command.

Help

Command	Argument
address-family	(A,B,C,D WORD) activate

BGP Basic

After entering each item and clicking the **[OK]** button, the setting values are displayed in the **<Current Status>** window.

BGP Basic

option	parameter
AS number	
neighbor	remote ☐ ebgp-multipath ☐ next-hop-self
network	/
redistribute	☐ connected ☐ static ☐ rip ☐ ospf

OK

Current Status

Displays the setting information related with BGP of GSIM. Click the **[Delete]** button to delete all setting information.

Current Status

Router BGP
router bgp 100
network 100.0.0.0/24

Delete

List

Access List

[List] → [Access List]

Access List

Access List

Option	Parameter
ID	Word test
Action	☒ Permit ☐ Deny
Source Match	☐ any ☒ Network 100 0 0 0 / 24
Exact match	☒ Exact match

OK

Item	Description
ID	Sets the Access-list name.
Action	Allows/Rejects the packet matched.
Source Match	Sets the match condition. – Any: All packets – Host: A host – Network: Network range
Destination Match	If ID ranges from 100 to 199 or from 2000 to 2699, Destination Match can be set as well as the Source Match condition. – Any: All packets – Host: A host – Network: Network range
Exac-match	Available when ID is set to word and when match condition is set to Network. Sets only the packets matched correctly with the prefix.

If the entered command is successfully executed, the execution result is directly applied to <Current Status> of [Layer3] → [List] → [Access List].

Current Status

This menu is used to retrieve the access list currently set in GSIM. Click the **[Delete]** button to delete the corresponding access-list.

Current Status

	ID	Entry
☒	test	permit 100.0.0.0/24 exact-match

Delete

Item	Description
ID	Access-list name information
Entry	Access-list description

Prefix List

[List] → **[Prefix List]** After setting the target item, click the **[Save]** button.

Prefix List

Option	Parameter
ID	
Seq	
Action	☒ Permit ☐ Deny
Prefix Match	☒ Any ☐ . . . / ge: le:

OK

Item	Description
ID	Sets the prefix-list name.
Seq	Sets the sequence No. of the prefix-list.
Action	Allows/Rejects the packets matched.
Prefix Match	Sets the match condition. - Any: All packets - Network: network range. Minimum and maximum prefix length can be set.

If the entered command is successfully executed, the execution result is directly applied to <Current Status> of [Layer3] → [List] → [Prefix List].

Current Status

Click the **[Delete]** button to delete the entry of the selected prefix list.

Click the **[Delete All]** button to delete all entries of the prefix list.

Current Status

	ID	Entry
☒	test	seq 5 permit 100.0.0.0/24

Delete
Delete All

Item	Description
ID	Prefix-list name information
Entry	Prefix-list information

Route-Map

[List] → [Route-Map] Enter the target value and click the **[Save]** button.

Route-Map

Option	Parameter
Name	test
Action	☒ Permit ☐ Deny
Sequence	1

OK

Item	Description
Name	Route-map name
Action	Sets whether to apply set operation.
Sequence	Sets the sequence No. to additionally delete a route-map

If the entered command is successfully executed, the execution result is directly applied to <Current Status> of [Layer3] → [List] → [Route-Map].

Route-Map Setting

	Name	Entry
☒	test	permit 10

Edit
Delete

Click the **[Delete]** button to delete the target route-map. Click the **[Edit]** button to modify the entry.

Item	Description
Name	Route-map name
Entry	Route-map information

Match & Set Operation

Match

Option	Parameter
☐ IP	☒ Address ☐ Use prefix-list ☐ Next-hop ☐ Use prefix-list
☐ Metric	

OK

Set

Option	Parameter
☐ IP	Next-hop
☐ Metric	
☐ Weight	
☐ Community	
☐ Metric-Type	Type-1
☐ Local Preference	

OK

Match Operation

Item	Description
IP	– Address: Sets the access-list or prefix-list for an IP to be matched. – Next-hop: Sets the Next-hop IP to be matched
Metric	Sets the Metric to be matched

Set Operation

Item	Description
IP	Sets the next-hop of the BGP table.
Metric	Sets the metric value of the BGP.
Weight	Sets the weight value of the BGP.
Community	Sets the community value of the BGP.
Metric-Type	Sets the metric type of the BGP. - Type 1 : External Type 1 - Type 2 : External Type 2
Local Preference	Designates the local preference among the BGP attributes.

Current Status

Click the **[Prev]** button to return to the route-map window mentioned above. Click the **[Delete]** button to delete the selected Match/Set operation.

Current Status

	Sequence	Entry
☐	10	match ip address test
☐	10	set ip next-hop 1.1.1.1

Item	Description
Sequence	Match/Set operation Sequence No. of route-map
Entry	Match/Set operation information of route-map

AS Path List

[List] → **[AS Path List]** Enter the target value and click the **[Save]** button.

AS path

Option	Parameter
ID	test
Action	☒ Permit ☐ Deny
Match	100\$

Item	Description
ID	Sets "AS Path" access-list name
Action	Sets permit/deny in the event that BGP route information exists that meets the match condition.
Match	Sets the match condition.

Current Status

This menu is used to display the information on the "As Path" access-list. Click the **[Delete]** button to delete the selected entry. Click the **[Delete All]** button to delete all of the access-list entries with the corresponding name.

Current Status

	ID	Entry
☒	test	permit 100\$

Item	Description
ID	"As Path" access-list name
Entry	"As Path" access-list information

Community List

Select **[List] → [Community List]** and set Community List. Set the target value and click the **[OK]** button.

Community List

Option	Parameter
ID	test
Action	☒ Expanded ☐ Standard
Match	☒ Permit ☐ Deny
	☒ No-Advertise

OK

Item	Description
ID	Sets Community list name – Expanded: When normally community list is set – Standard: When a community list with the selected format is set
Action	Sets whether to allow/reject the community to be matched
Match	– No-Advertise: Do not distribute the path to the neighbor router – No-Export: Do not distribute the path to an external neighbor router – Local-AS: Do not distribute path to the neighbor router of the lower AS located at BGP combination network.

If the entered command is successfully executed, the execution result is directly applied to **<Current Status>** of **[Layer3] → [List] → [Community List]**.

Current Status

Click the **[Delete]** button to delete the target community-list entry. Click the **[Delete All]** button to delete all community-list entries.

Current Status

ID	Entry
expanded test	permit no-advertise

Delete

Delete All

Item	Description
ID	Community list name
Entry	Community list information

Status

RIP

This menu is used to display RIP connection status and information.

Item	Description
Network	Displays network information
Next Hop	Next-hop address of the RIP route.
Metric	Metric information
From	Displays the address being connected.
If	Displays interface information.
Time	Update time

OSPF

This menu is used to check the OSPF connection status and information with the other routers.

OSPF Information

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.17.101	1	Full/Backup	00:00:37	30.0.1.1	rd2

Refresh

Item	Description
Neighbor ID	Neighbor ID of the other router
Pri	Priority
Status	Displays the connection process
Dead Time	Displays the dead time.
Address	Address of the other party
Interface	Interface connected

BGP

This menu is used to check the BGP connection status information and BGP routing table information.

BGP Information

Category	Value
BGP Router ID	192.168.0.98
Local AS Number	100
BGP Table Version	1
BGP AS-PATH Entries	1
BGP Community Entries	0
Total Neighbor	1

Item	Description
BGP Router ID	BGP Router ID is the tie-breaker for the BGP path selection. The path selection process uses a variety of metrics to select a route. If all other metrics (accessibility, administrative weight, local preference, etc.) are equal, BGP determines the router ID using the following priority
Local AS Number	Local AS No. set by a user
BGP Table Version	BGP table change version information
BGP AS-PATH Entries	Number of AS-PATH Hash tables used in BGP
BGP Community Entries	Number of Hash table of community attribute used in BGP
Total Neighbor	Total sum of BGP neighbor

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
192.168.0.1	4	100	0	0	0	0	0	never	Idle

Item	Description
Neighbor	IP address of the neighbor router
V	Version No. used by neighbor
AS	AS No. of neighbor
MsgRcvd	Message number received from neighbor
MsgSent	Message number sent from neighbor
TblVer	Latest BGP database version sent from neighbor
InQ	Number of messages that should be received from neighbor and processed
OutQ	Number of messages sent to neighbor

Item	Description
Up/Down	Displays the path time when BGP the session is finished. Displays the status when BGP the session is not finished.
State/PfxRcd	Number of BGP routes via neighbor or peer group or BGP current status

Network	Nexthop	Metric	LocalPrf	Weight	Path
* > 100.0.0.0/24	0.0.0.0			32768	i
Refresh					

Item	Description
Network	Displays network information. Status code information – s: Indicates the suppressed network. – *: Indicates proper network information. – h: BGP dampening is activated. – >: best route – i: Indicates the network entered by IBGP.
Nexthop	Next-hop address of the BGP route sent from neighbor
Metric	MED value of BGP neighbor
LocalPrf	Local Preference. Default is 100.
Weight	Weight allocated in prefix Local route default is 32768. The default of the sent route is 0.
Path	Displays the list of AS-Path that should be passed to go to the network corresponding to the prefix. Origin code information – i: Information received by the network command – e: Information received via EGP – ?: Information received by redistribution

IPMC

Select the **[IPMC]** menu. The submenus will be displayed in the upper left side of the window as follows:

IPMC
General
Mroutes
Management
Configuration
IGMP
DVMRP
DVMRP Intf
PIM-SM
PIM-SM Intf
Status
IGMP Groups
DVMRP
PIM-SM

Menu	Submenu	Description
General	Mroutes	Displays Multicast Routing Entry.
	Management	Starts/Stops IPMC protocol daemons.
Configuration	IGMP	Displays or changes IGMP setting.
	DVMRP	Displays or changes DVMRP default setting.
	DVMRP Intf	Displays or changes VIF of DVMRP.
	PIM-SM	Displays or changes PIM-SM default setting.
	PIM-SM Intf	Displays or changes VIF PIM-SM.
Status	IGMP Groups	Displays IGMP Group information.
	DVMRP	Displays DVMRP neighbor and Prune information.
	PIM-SM	Displays PIM-SM Neighbor information.

General

Mroutes

Mroute	Uptime	Expires	Flags	Incoming	Outgoing
(100.1.1.11, 224.1.1.100)	00:00:08	00:03:22	TF	rd2	rd3

I: Immediate Stat, T: Timed Stat, F: Forwarder installed

Clear Refresh

Item	Description
Mroute	Multicast Routing identifier
Uptime	Past time after starting the operation of multicast routing entry
Expires	Rest time until multicast routing entry is expired
Flags	Multicast routing characteristic flag. Refer to the description on the lower part.
Incoming	Name of VIF to which multicast is sent
Outgoing	List of VIF where multicast is sent

Management

This menu is used to execute or stop dvmrpd and pimd, IPMC protocol demons. **[Current Status]** of Management shows the current status of each demon. To change the demon status, select another status from the combo box of **[Action]** and click the **[OK]** button.

Protocol	Current Status	Action
DVMRP	Stop	On
PIM	Stop	Off

OK

Item	Description
Protocol	IPMC protocol
Current Status	Current IPMC protocol demon status
Action	New status of IPMC protocol demon status

Configuration

IGMP

This menu is used to display and change IGMP setting.

IGMP & Help

IGMP command can be entered and executed. Command that can be executed can be retrieved in the following Help table. Enter the target command into the input field of IGMP and click the **[OK]** button. Then, the command is executed.

IGMP

Command

OK

Help

Command	Argument
clear ip igmp	group

IGMP Basic

Enter new information and click the **[OK]** button to change the default setting of IGMP.

IGMP Basic

Command	Argument
Interface	☒ All ☐ eth0 (192.168.17.100/16)
IGMP Query Interval	125 (1~65535, Default: 125)
Max Response Time	10 (1~25, Default: 10)

OK

Item	Description
Interface	Selects the target IGMP interface and select All. Then, all interface-setting values are applied.
IGMP Query Interval	Cycle for sending IGMP Membership Query.
Max Response Time	Maximum time of waiting for a response after sending Membership Query.

IGMP Interface Information

This menu is used to display the setting values of IGMP interfaces.

IGMP Interface Information				
Address	Intf	Querier Address	Query Interval	Max Resp Time
100.1.2.10/24	rd2	100.1.2.10/24	125	10
100.1.3.10/24	rd3	100.1.3.10/24	125	10

Item	Description
Address	IGMP group address
Intf	IGMP interface name
Querier Address	IP address of IGMP interface that sends membership query. IP address of Designate Router(DR).
Query Interval	Cycle of sending Membership Query.
MaxResp Time	Maximum time of waiting a response to Membership Query.

DVMRP

This menu is used to set DVMRP, a IPMC protocol. In addition, the Route items of DVMRP being operated can be displayed.

DVMRP & Help

Commands can be executed to set DVMRP. The commands that can be executed in Help can be searched. Enter a command into DVMRP and click the **[OK]** button to execute the command.

DVMRP

Command

OK

Help

Command	Argument
clear ip dvmrp	route A.B.C.D/M

DVMRP Routes

This menu is used to display DVMRP Route items being used.

DVMRP Routes						
Source Network	Flags	Intf	Neighbor	Metric	Uptime	Expires
100.1.2.0/24	.D.	rd2	Directly Connected	1	00:05:10	00:00:00
100.1.3.0/24	.D.	rd3	Directly Connected	1	00:05:05	00:00:00
Refresh						

Item	Description
Source Network	VIF network address to which multicast packets flow.
Flags	DVMRP route feature flag. N=New, D=Direct Connected, H=Hold down
Intf	VIF name to which multicast packets flow.
Neighbor	DVMRP neighbor IP address that provides information on DVMRP route.
Metric	DVMRP route Metric(=distance) value.
Uptime	Time passed after using the DVMRP route item.
Expires	Time left until the DVMRP route item is expired.

DVMRP Intf

This menu is used to add or set DVMRP VIF.

RD Interface

This menu is used to add L3 interface where an IP address is set to DVMRP VIF. Select the target interface to be added to VIF from the Interface item, enter the target value, and click the **[Add]** button.

RD Interface	
Command	Argument
Interface	eth0 (192.168.17.100/16)
Reject Non-pruners	☐ (do not allow old version DVMRP neighbors)
Metric	1 (1~31)
Add	

Item	Description
Interface	Select the target L3 interface.
Reject Non-pruners	Non-pruners indicate the neighbors that only support DVMRP with the previous version. Mark if this is not communicated with the DVMRP with the previous version.
Metric	Metric(=distance) value to be used for multicasting routing by VIF.

DVMRP Interfaces

This menu is used to display the setting DVMRP VIF. To delete a specific VIF, check the check box on the left and click the **[Delete]** button.

DVMRP Interfaces					
	Intf	Address	Type	Neighbor Count	Remote Address
☐	rd2	100.1.2.10/24	BCAST	1	N/A
☐	rd3	100.1.3.10/24	BCAST	0	N/A

Item	Description
Intf	DVMRP VIF name.
Address	IP address of DVMRP VIF.
Type	DVMRP VIF type. Tunnel, Point-to-Point, Broadcast.
Neighbor	Number of neighbors connected to DVMRP VIF.
Remote Address	Address of the other party in case of Tunnel or Point-to-Point type. Peer Address

PIM-SM

This menu is used to set PIM-SM.

PIM-SM & Help

Command can be executed to set PIM-SM. Commands that can be executed can be retrieved in Help. Enter the target command into the input field of PIM-SM and click the **[OK]** button.

PIM-SM

Command

clear ip pim sparse-mode bsr rp-set *

OK

Help

Command	Argument
clear ip pim	sparse-mode bsr rp-set *

PIM-SM Basic

This menu is used to set BSR and RP of PIM-SM protocol. Mark the check box on the right and enter the setting values. Click the **[OK]** button to apply the values. If deleting the set value, check in the checkbox of the relevant set items, and click [Delete] button.

PIM-SM Basic

	Command	Argument
☒	RP Address	192 . 168 . 17 . 100
☒	RP Candidate	rd1 22 Priority(0~255)
☒	BSR Candidate	rd1 30 MaskLen(0~32) 100 Priority(0~255)

OK

Delete

Refresh

Item	Description
RP Address	When setting static RP, enter the IP address of RP.
RP Candidate	When setting RP Candidate, select VIF and enter the target priority. (Small value has high priority.)
BSR Candidate	When setting BSR Candidate, select VIF and enter the target Mask Length and Priority. (High value has high priority.)

BootStrap Information

This menu is used to display BootStrap information.

BootStrap Information

PIMv2 Bootstrap information

This system is the Bootstrap Router (BSR)

BSR address: 10.0.3.1

Uptime: 00:00:04, BSR Priority: 100, Hash mask length: 30

Expires: 00:02:06

Role: Candidate BSR

State: Pending BSR

Candidate RP: 10.0.3.1(rd1)

Advertisement interval 60 seconds

Next Cand_RP_advertisement in 00:00:58

Refresh

RP Information

This menu is used to display the RP information.

RP Information

PIM Group-to-RP Mappings

This system is the Bootstrap Router (v2)

Group(s): 224.0.0.0/4

RP: 10.0.3.1

Info source: 10.0.3.1, via bootstrap, priority 22

Uptime: 00:18:40, expires: 00:01:50

Group(s): 224.0.0.0/4, Static

RP: 192.168.17.100

Uptime: 00:19:00

Refresh

PIM-SM Intf

This menu is used to set PIM-SM VIF.

RD Interface

This menu is used to add PIM-SM VIF. Select the target L3 interface from the Interface item, enter the target values, and click the **[Add]** button to add PIM-SM VIF.

RD Interface

Command	Argument
Interface	eth0 (192.168.17.100/16)
Mode	Sparse
DR Priority	1 (0~4294967294)
Hello Interval	30 (1~65535)

Add

Item	Description
Interface	Selects the target L3 interface to be added to PIM-SM VIF
Mode	Selects the target PIM-SM protocol mode. Sparse, Passive
DR Priority	Enters the priority value used when selecting Designate Router (DR). (High value has high priority.)
Hello Interval	Cycle of exchanging hello packets with connected PIM-SM neighbors.

PIM-SM Interfaces

This menu is used to display the VIFs added to PIM-SM. To delete a VIF, click the check box on the left and click the **[Delete]** button.

PIM-SM Interfaces							
	Intf	Address	Mode	Neighbor Count	DR Prio	DR	Hello Intv/Hold
☐	rd2	100.1.2.10/24	Sparse	0	1	100.1.2.10	30/105
☐	rd3	100.1.3.10/24	Sparse	0	1	100.1.3.10	30/105

Status

IGMP Groups

This menu is used to display information on registered IGMP groups.

IGMP Group Information				
Group Address	Intf	Uptime	Expires	Last Reporter
224.1.1.100	rd3	00:00:03	00:04:17	100.1.3.31

Item	Description
Group Address	IGMP group address.
Intf	IGMP interface name.
Uptime	Time passed after IGMP group is created.
Expires	Time left until the IGMP Group information is expired.
Last Reporter	Client IP address that sends the last membership report.

DVMRP

This menu is used to display the DVMRP protocol status.

DVMRP Neighbors

This menu is used to display the information on the DVMRP neighbor whose information is exchanged.

DVMRP Neighbors			
Neighbor Address	Interface	Uptime	Expires
100.1.2.1	rd2	00:02:04	00:00:31
Refresh			

Item	Description
Neighbor Address	IP address of DVMRP Neighbor.
Interface	DVMRP VIF name.
Uptime	Time passed after being connected.
Expires	Time left until the Neighbor connection information is expired.

DVMRP Prune Information

This menu is used to display DVMRP Prune items.

DVMRP Prune Information						
Source Address	MaskLen	Group Address	State	FCR Cnt	Expires	ReXmit
100.1.1.0	24	224.1.1.100		0	01:59:06	Off
P: Pruned, H: Host, D: Holddown, N: NegMFC, I: Init						
Refresh						

Item	Description
Source Address	Host IP address that sends multicast packets
MaskLen	Mask length of DVMRP Prune
Group Address	Multicast group address
State	Flags that display the DVMRP Prune status. Refer to the description on the lower side
FCR Cnt	DVMRP Forwarding Cache count
Expires	Time passed after the DVMRP Prune information is created
ReXmit	Time left until retransmission

PIM-SM

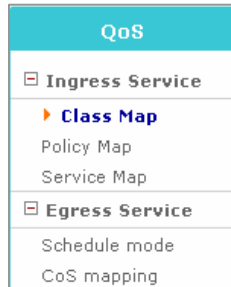
This menu is used to display the neighbor list of PIM-SM protocol.

PIM-SM Neighbors						
Neighbor	Intf	Uptime	Expires	Ver	DR Priority	DR
100.1.2.1	rd2	00:02:17	00:01:29	v2	1	.
Refresh						

Item	Description
Neighbor	Neighbor IP address
Intf	IP address of VIF connected with neighbor
Uptime	Time passed after being connected with neighbor
Expires	Time left until the Neighbor connection information is expired
Ver	Version of the PIM-SM protocol used for the connection
DR Priority	Designate Router(DR) priority of neighbor
DR	Displays whether the neighbor is Designate Router(DR)

QoS Menu

Select the **[QoS]** menu. The submenus will be displayed in the upper left side of the window as follows.



Menu	Submenu	Description
Ingress Service	Class Map	Generates, modifies and deletes a class map.
	Policy Map	Generates, modifies and deletes a policy map.
	Service Map	Applies a policy map set up at each port.
Egress Service	Schedule Mode	Sets up scheduling method to each port.
	CoS mapping	Sets up CoS queue mapping of each port.

Ingress Service

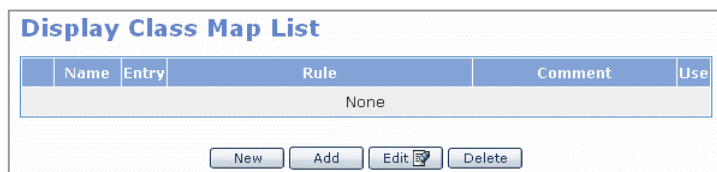
The ingress function manages desired traffic by filtering inbound traffic and can manage traffic that exceeds the established traffic volume by measuring the traffic volume.

To set up QoS, three steps are required as follows:

1. Generate a class map to filter a packet to apply QoS.
2. Generate a policy map to activate a packet that a class map has filtered.
3. Select the target port and apply the policy map to the port.

Class map

The class map generates a rule to filter incoming packets. The class map can set up multiple fields from the MAC address of Layer2 to the TCP/UDP port of Layer4 simultaneously.



Press the **[New]** button to generate new class map.

New Class Map

Category	Value
Name	
Comment	
Destination MAC	: : : : :
Source MAC	: : : : :
802.1p Priority Tag	None
VLAN Tag	(1~4094)
Ethernet Type	0x (Hex format)
ICMP Type	None
IP Protocol	(0~255) None
Destination IP	. . . /
Source IP	. . . /
Diffserv Code Point	(0~63)
Destination Port	None Range
Source Port	None Range

OK Cancel

Item	Description
Name	Name of new class map to be generated. The item cannot be modified when editing the name of the class map. (Alphanumeric characters 1~20 long)
Comment	Simple description for class map. (Alphabetical characters 0~128 long)
Destination MAC	Destination Address of MAC. It is composed of three fields in the method of ZebOS and each field is configured with 4 hexadecimal digits.
Source MAC	Source Address of MAC. The input type is the same as Destination MAC.
802.1p Priority Tag	802.1p Priority Tag(0~7 values)
VLAN Tag	VLAN tag(1~4094)
Ethernet Type	Hexadecimal value(2-byte)
ICMP Type	(0~18)
IP Protocol	(0~255)
Destination IP	Configured with four fields and prefixes. (Four fields between 0~255, Prefix between 0~32)
Source IP	Same as the destination IP.
Diffserv Code Point	(0~63)
Destination Port	Values between 0~65534 or 1~65536. It is in the form of a multiple of 2 when having a range value
Source Port	Same as the destination port.

The following is an example that filters the value that the priority value is 3 for the source MAC 00:00:00:00:00:01 and 802.1p. Press the **[OK]** button to generate class1.

New Class Map

Category	Value
Name	class1
Comment	This is class1
Destination MAC	: : : : :
Source MAC	00 : 00 : 00 : 00 : 00 : 01
802.1p Priority Tag	3
VLAN Tag	(1~4094)
Ethernet Type	0x (Hex format)
ICMP Type	None
IP Protocol	(0~255) None
Destination IP	. . . /
Source IP	. . . /
Diffserv Code Point	(0~63)
Destination Port	None Range
Source Port	None Range

OK Cancel

The following is an example that the source IP network and destination port are set up. Press the **[OK]** button to generate class2.

New Class Map

Category	Value
Name	class2
Comment	This is class2
Destination MAC	: : : : :
Source MAC	: : : : :
802.1p Priority Tag	None
VLAN Tag	(1~4094)
Ethernet Type	0x (Hex format)
ICMP Type	None
IP Protocol	(0~255) None
Destination IP	. . . /
Source IP	192 . 168 . 0 . 0 / 24
Diffserv Code Point	(0~63)
Destination Port	80 None Range
Source Port	None Range

OK Cancel

Two classes are generated as shown above. The value of “Use” is 0 since no policy map has been used.

Display Class Map List

	Name	Entry	Rule	Comment	Use
☐	class2	1	ip-source-address 192.168.0.0/24 ip-destination-port 80	This is class2	0
☐	class1	1	mac-source-address 0000.0000.0001 prio-tag 3	This is class1	0

Select the desired class map and press the **[Add]** button to generate an additional entry to the generated class map. Only the fields related to the class map is displayed. Fill in the fields and press the **[OK]** button.

Add Class Entry

Category	Value
Entry Number	2
ip-source-address	192 . 168 . 1 . 0 / 24
ip-destination-port	24 None Range

The class map currently set up is displayed as Display Class Map List.

Display Class Map List

	Name	Entry	Rule	Comment	Use
☐	class2	1	ip-source-address 192.168.0.0/24 ip-destination-port 80	This is class2	0
☐		2	ip-source-address 192.168.1.0/24 ip-destination-port 23		
☐	class1	1	mac-source-address 0000.0000.0001 prio-tag 3	This is class1	0

Edit class

Select the desired class map or entry and press the **[Edit]** button to modify the value of a class map or the value of class entry. Press the **[Delete]** button to delete a class map or class entry that is already generated. If selecting a class map, all entries of the class map are all deleted. If the value of Use is higher than 0, it cannot be deleted.

Policy Map

The policy map activates filtered packets. In addition, multiple class maps can be applied and the policy map adjusts the priority values between them.

The priority is applied to the action of higher values when being identical to all class maps set up by a packet. The default class of the policy map executes the basic action of packets that are not included in the class map.

Display Policy Map List

Name	Class	Seq	Entry	Action	Comment	Use
None						

Press the **[New]** button to generate new policy map.

New Policy Map

Category	Value
Name	
Comment	
Default-class	None v
class1	None v
class2	None v

Each item is defined as follows:

Item	Description
Name	Name of new policy map to be generated. The item cannot be modified when editing the name of the class map. (Alphanumeric characters 1~20 long)
Comment	Simple description for the policy map.(Alphabetical characters 0~128 long)
Default-class	Designates basic action for the packets that are not identical with all class map set up to the policy map.
Class-list	Displays the class map list that sets up in class map.
sequence	Has a value between 10 and 15. The priority is assigned to according to the size of the value.

The following is an example of the generation of a map, policy1, set up class1 to 15 and class2 to 14. The default-class is usable as it is set up as shown below.

New Policy Map

Category	Value
Name	policy1
Comment	This is policy1
Default-class	Use ☐
class1	Sequence 15 ☐
class2	Sequence 14 ☐

OK Cancel

Press the **[OK]** button to generate a policy map, policy1.

Display Policy Map List

	Name	Class	Seq	Entry	Action	Comment	Use
☐		class1	15	1	Conform action clauses: permit	This is policy1	0
☐	policy1	class2	14	1	Conform action clauses: permit		
☐		default	0		Conform action clauses: permit		

New Edit  Active Delete

Press the **[Edit]** button to modify the priority or remove the class map set up to the policy map.

Select the class map or entry set up to the policy map and press the **[Active]** button to add, modify or delete the action of the class map.

Conform Action

	Category	Value
☒	permit	
☐	deny	
☐	copy-to-mirror	
☐	increase-counter	
☐	tos-to-priority	
☐	priority-to-tos	
☐	drop-precedence	
☐	set-out-port-ucast	None ☐
☐	set-out-port-non-ucast	None ☐
☐	set-out-port-all	None ☐
☐	insert-vlanid	(1~4094)
☐	insert-priority	None ☐
☐	set-priority	None ☐
☐	insert-tos	None ☐
☐	insert-dscp	None ☐
☐	set-ecn	None ☐

Conform Action is an action that can be executed when the class map is identical regardless of the bandwidth of a packet.

Item	Description
permit	Switches a packet.
deny	Drops a packet without switching.
copy-to-mirror	Copies a packet to the port when a mirror port is set up.
increase-counter	Increases internal counter.
tos-to-priority	Sets up the value of ToS precedence 3bit of the IP header to the value of 802.1p.
priority-to-tos	Sets up the value of 802.1p to the value of ToS precedence 3bit of the report IP header.
drop-precedence	The packets that the action is set up are drops preferentially when congestion occurs in an egress.
set-out-port-ucast	Redirects a unicasted packet to an established port.
set-out-port-non-ucast	Redirects a packet that is not an unicast to an established port.
set-out-port-all	Re direct to an established port for all packets.
insert-vlanid	Changes the value of VLAN ID to the established value.
insert-priority	Changes the value of 802.1p to the established value.
set-priority	Sets up the priority of packets internally.
insert-tos	Changes the value of ToS to the established value.
insert-dscp	Changes the value of DSCP to the established value.
set-ecn	Changes the value of ECN to the established value.

Exceed Action sets up the action for packets exceeding the established rate-limit bandwidth.

Exceed Action		
	Category	Value
☐	rate-limit	limit : Kbps burst : Kbit
☐	permit	
☐	deny	
☐	drop-precedence	
☐	insert-dscp	None ▼
☐	set-ecn	None ▼

Item	Description
rate-limit	- limit: The value of a bandwidth to apply exceed-action. - burst: The value of burst to apply exceed-action.
permit	Switches a packet.
deny	Drops a packet without switching.

Item	Description
drop-precedence	A packet that an action is set up is dropped preferentially when congestion occurs.
insert-dscp	Changes the value of DSCP to the established value.
set-ecn	Changes the value of ECN to the established value.

Conform Action or Exceed Action performs multiple actions and ‘permit’ and ‘deny’ is set up exclusively. In the following example, Conform Action is set up as traffic exceeding 500Mbps are denied when the value of dscp is 3 for the packets included in the class1 and the internal priority is 7.

Conform Action

	Category	Value
☒	permit	
☐	deny	
☐	copy-to-mirror	
☐	increase-counter	
☐	tos-to-priority	
☐	priority-to-tos	
☐	drop-precedence	
☐	set-out-port-ucast	None ▼
☐	set-out-port-non-ucast	None ▼
☐	set-out-port-all	None ▼
☐	insert-vlanid	(1~4094)
☐	insert-priority	None ▼
☒	set-priority	7 ▼
☐	insert-tos	None ▼
☒	insert-dscp	3 ▼
☐	set-ecn	None ▼

Exceed Action

	Category	Value
☒	rate-limit	limit : Kbps burst : Kbit
☐	permit	
☒	deny	
☐	drop-precedence	
☐	insert-dscp	None ▼
☐	set-ecn	None ▼

After the setup above, the window is displayed as follows:

Display Policy Map List							
	Name	Class	Seq	Entry	Action	Comment	Use
☐	policy1	class1	15	1	Conform action clauses: permit set-priority 7 insert-dscp 3 Exceed action clauses: rate-limit 500000 20000 deny	This is policy1	0
☐		class2	14	1	Conform action clauses: permit		
☐		default	0		Conform action clauses: permit		

Service Policy

Even multiple class maps and policy maps are set up, this setup is not applied to the switch directly. To apply the setup to the switch, select the desired policy map of each port from Service Policy.

Service Policy			
Port	Policy Map	Port	Policy Map
Port 1	None	Port 6	None
Port 2	None	Port 7	None
Port 3	policy1	Port 8	None
Port 4	policy2	Port 9	None
Port 5	None	Port 10	None

Item	Description
Port	Port Number of Switch
Policy Map	Established policy map name or establishable policy map list

If selecting a policy map currently made from Policy Map, the policy map is applied to the relevant map, and select None not to apply QoS to the port.

Egress Service

Egress Service performs scheduling functions for traffic transferred from the switch according to each Q and mapping packets by transferring each packet to the desired Queue according to its priority, as there are 8 internal Queues per each port in Egress.

Schedule Mode

There are 3-Schedule Modes. Strict priority, round robin and weighted round robin. The weighted round robin mode can set the value of weight according to each Q.

Schedule Mode

Port	Mode	Weight							
Port 1	weighted-round-robin	q0	0	q1	0	q2	0	q3	0
		q4	0	q5	0	q6	0	q7	0
Port 2	weighted-round-robin	q0	0	q1	0	q2	0	q3	0
		q4	0	q5	0	q6	0	q7	0
Port 3	weighted-round-robin	q0	0	q1	0	q2	0	q3	0
		q4	0	q5	0	q6	0	q7	0
Port 4	weighted-round-robin	q0	0	q1	0	q2	0	q3	0
		q4	0	q5	0	q6	0	q7	0
Port 5	weighted-round-robin	q0	0	q1	0	q2	0	q3	0
		q4	0	q5	0	q6	0	q7	0
Port 6	weighted-round-robin	q0	0	q1	0	q2	0	q3	0
		q4	0	q5	0	q6	0	q7	0
Port 7	weighted-round-robin	q0	0	q1	0	q2	0	q3	0
		q4	0	q5	0	q6	0	q7	0
Port 8	weighted-round-robin	q0	0	q1	0	q2	0	q3	0
		q4	0	q5	0	q6	0	q7	0
Port 9	weighted-round-robin	q0	0	q1	0	q2	0	q3	0
		q4	0	q5	0	q6	0	q7	0
Port 10	weighted-round-robin	q0	0	q1	0	q2	0	q3	0
		q4	0	q5	0	q6	0	q7	0

OK

Item	Description
Port	Port Number of Switch
Mode	Schedule Mode(strict-priority, round-robin, weighted-round-robin)
Weight	It is available to set up with activated for weighted round robin.

CoS Mapping

Packets are transferred to each Q according to the priority(0~7). Basically, the priority 0 is mapped to Q 0 and the priority 7 is mapped to Q 7 sequentially. The following shows a window that the packet of Priority 3 is changed to Q 4 instead of Q 3 in Port3.

CoS Mapping

Port	Priority	Queue	Priority	Queue
Port 3	0	0	4	4
	1	1	5	5
	2	2	6	6
	3	4	7	7

Queue	Threshold	Queue	Threshold
0	128	4	128
1	128	5	128
2	128	6	128
3	128	7	128

Each Q has its own threshold. If a value that is higher than the threshold is led into the Q, the value is dropped.

Item	Description
Port	Port Number of Switch
Priority	Priority Value(0~7) of packet
Queue	Q(0~7) to serve packet
Threshold	Threshold(0~2048) to set up each Q(0~2048)

Application Menu

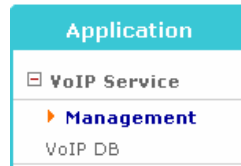
Select the **[Interface]** menu. The submenus will be displayed in the upper left side of the window as follows.

Application
VoIP Service
Management
VoIP DB
DHCP Server
Configuration
Management
Lease Info
DHCP Relay Agent
Configuration
Management

Menu	Submenu	Description
VoIP Service	Management	Able to start or stop the functions of the VoIP Service.
	VoIP DB	Displays the information of the OfficeServ 7400 systems that has been received until now.
DHCP Server	Configuration	Sets configuration items of DHCP Server.
	Management	Manages the operation of DHCP Server.
	Lease Info	Verifies the status of DHCP Server.
DHCP Relay Agent	Configuration	Configures DHCP Relay by registering interface and DHCP server.
	Management	Executes/Stops DHCP Relay Demon by applying the DHCP Relay setup.

VoIP Service Menu

Select the **[Application]** menu. The submenus will be displayed in the upper left side of the window as follows:



Management

In the [Management] menu, the function of the VoIP Service can start or stop. Although the system is rebooted, the system is recovered into the status stored in the latest.

VoIP Service Management	
Activity	Action
Running	Stop

Item	Description
Activity	The status of the current VoIP Service.
Action	The command that can be executed in the current status.

VoIP DB

[VoIP DB] menu displays the information of the OfficeServ 7400 systems that has been received until now.

VoIP Database				
Call Server		Status	IP	MAC Address
MCP		Connected	165.213.176.10	00.00.f0.ff.74.49
MGI Cabinet	Slots	Status	IP	MAC Address
ITP Index	Status	IP	TEL NUM	MAC Address
WIP Index	Status	IP	TEL NUM	MAC Address
Refresh				

Item	Description
Call Server	Indicates the categories of the Call Server (7200/7400)
Status	Indicates the status of each card and the phone.
IP	Indicates each card and the IP of the phone.
MAC Address	Indicates each card and the Phone MAC Address
MGI Slots	Indicates the slots of the MGI card.
ITP Index	Indicates the index of the ITP Phone.
WIP Index	Indicates the index of the WIP Phone.
Port	Indicates the ports of the ITP/WIP Phone.
TEL NUM	Indicates the phone numbers of the ITP/WIP Phone.

DHCP Server

[DHCP Server] → [System] enables or disables the DHCP daemon.

Configuration

The [Configuration] menu allows setting various configuration items of DHCP Server. Basically, Pool Name, Network Address and Range Address are the required fields in DHCP Server setup.

General Options

Parameter	Argument
* Pool Name	
* Network Address	. . . /
* Range Address	. . . ~ . . .
Lease Time	1 Days 0 Hours 0 Minutes ☐ Infinite
Group Number	
Client ID	
Vendor ID	
Domain Name	
Default-Router	. . .
Fixed Address	Host
	MAC : : : : :
	IP . . .
DNS Server	1) . . . 2) . . .
WINS Server	1) . . . 2) . . .

Current Running Configured Information

Select	Parameter	Argument
No Entry		

The setup of DHCP Server is configured by Pool. Each item is described as follows:

Item		Description
* Pool Name		Sets up the name of Pool to distinguish from the other Pools.
* Network Address		The value of a Network to be set up. The value is classified by IP type and Netmask.
* Range Address		Sets up the range of IP address that DHCP Server allocates to DHCP Client. Enter the first/last IP addresses to be allocated in order to designate the range.
Lease Time		Sets up the duration to lease an IP address to DHCP Client. The default is 1 day.
Client ID		Sets up Client Identifier.
Vendor ID		Sets up Vendor Class Identifier.
Domain Name		Sets up Domain Name.
Default-Router		Sets up IP address of Default Router.
Fixed Address	Host	Sets up Name of Host.
	MAC	Sets up MAC address of a specific client.
	IP	Sets up IP Address to be allocated.
DNS Server		Sets up DNS Server.
WINS Server		Sets up WINS Server.

Fixed Address is used for allocating a fixed IP address for a specific client.

If pressing **[Save]** button after the setup, the setup is saved. It is available to verify and delete the saved information in the table below.

Press the **[Delete]** button after checking the target Pool in order to delete. Check the pool that is to be corrected, and press **[Edit]** button if correcting.

Management

This function manages the operation of DHCP Server.

It is available to verify the status of DHCP Server and operate/stop DHCP Server Demon using the **[Run/Stop]** button.

DHCP Server Management	
Status	Action
Stop	Run

Lease Info

Lease Info is a window that allows verifying the status of DHCP Server.

DHCPD Demon operates according to the setup after reading the setup from the setup file, and records the information on allocation or returned IP Address to a specific file. Lease Info extracts the information on such file to display on the window.

Lease Info displays the information on the allocated IP Address and information used for the setup of the window and DHCP Server.

DHCP Leases Usage

Pool Name	Network	Total	Used	Usage
-----------	---------	-------	------	-------

DHCP Leases Information

IP	MAC	Lease Starts	Lease Ends
----	-----	--------------	------------

DHCP Relay Agent

DHCP Relay Agent is used for applying one DHCP server to multiple Subnets. Therefore, when DHCP Server and DHCP Client are in different networks from each other, the DHCP Client allows allocating an IP from IP.

Configuration

DHCP Relay Agent can be built by assigning an interface to be relayed and registering DHCP Server in the Configuration menu.

Designating an interface, which is relayed, from the list of the activated interfaces by using the **[Add]** button. Then the list for the designated interface is configured and, if pressing the **[Delete]** button from the list, the interface is deleted.

To save the list of DHCP Server, enter the IP address that is DHCP Server is operating and adds the address. To delete the list, select a DHCP Server to be deleted and press the **[Delete]** button.

Interface List Configuration

Check	Argument
	RD 1

Add
Delete

Check	Server List	Server
	Server List	. . .

Add
Delete

Management

This function operates and stops the configured DHCP Relay. It is composed of the status display of DHCP Relay Demon and **[Run/Stop]** button.

DHCP Relay Agent Management	
Status	Action
Stop	Run

System Menu

Select the **[System]** menu. The submenus will be displayed in the upper left side of the window as follows.

System
DB Config
Admin Config
Log
Configuration
Report
Download
Time Config
NTP Config
Manual Config
Timezone
Upgrade
Appl Server
Reboot

Menu	Submenu	Description
DB Config	-	Stores DB to PC or modifies DB into the DB file of PC to modify Default DB.
Admin Config	-	Sets up for the management authentication.
Log	Configuration	Sets up to determine whether to leave the log for each item.
	Report	Retrieves the system log currently stored.
	Download	Downloads System Log.
Time Config	NTP Config	Sets up Time Server to synchronize the information on the time server, date and time.
	Manual Config	Sets and modifies the date and time of the system to the time that the user wants.
	Timezone	Changes the timezone by selecting the timezone related to the user.
Upgrade	-	Upgrades Kernel and Ramdisk.
Appl Server	-	Performs TELNET, FTP and SSH services to connect with the GSIM board remotely.
Reboot	-	Reboots the system.

DB Config

The **[DB Config]** menu stores DB and changes to the basic DB or user DB.

Configuration System DB

Select	Type	Description
☒	Import	Browse...
☐	Export	Export the current system db.
☐	Default	Change the current system db to default system db.

[OK](#)

item	Description
Import	Modifies to DB that exists on the user's PC.
Export	Stores the DB in use to the user's PC.
Default	Modifies DB to initial setup.

To modify DB using the DB Import function, the DB file should be stored on PC in advance. As the DB default is changed to the initial DB, the web manager should be connected to 10.0.3.1 through the LAN port of the internal network after the restart of the system.

Admin Config

This function sets up the authentication server of the system login. It sets up the Local, Radius and Taccas + authentication server. Select the authentication mode that is to be used, and click **[OK]** button. Then its application is applied, and the page set for the selected application mode is displayed.

Login Policy

Category	Value
Set Policy	☒ Local ☐ Radius ☐ Taccas+

[OK](#) [Cancel](#)

Local

Change the Local Password. Enter new password and click the **[OK]** button to change the Local Password of the system.

Local

Category	Configuration
New Password	
Confirm New Password	

[OK](#)

Radius

Enter the information on the Radius authentication server. If entering Server IP, key defined on Server and timeout time and clicking the **[Add]** button, the entered values are applied to the system. Up to 5 lists can be entered. If checking the entered lists and pressing the **[Delete]** button, the selected lists are deleted.

Radius

Radius Server IP	Radius Server Key	Time out

Add
Delete

Taccas+

Enter the information on the Taccas+ authentication. Up to 5 lists are entered or deleted the same as the Radius input page. All of server Ip addresses and secret keys should be entered initially. The secret key can be renewed when values are added. The secret key values are cleared when all server IP lists are deleted.

Taccas+

Taccas+ Server

Taccas+ Secret Key

Add
Delete



CAUTION

Setup Application

Login Policy should be applied first to activate the server authentication to the system. If entering the authentication information in the status that the Logging Policy is only selected without application, the information is not applied to the server authentication information.

Log

This page allows setting up the system log and retrieve the information.

Configuration

This page allows setting up the log to determine whether to add a log to the system.

Log Policy

Advanced Service		
Log	ON ☒	OFF ☐

Determine to add a log to the system and click the **[OK]** button to add the log to the system log. Click the **[Reset]** button before applying the setup to return to the previous status.

Log Report

This window allows retrieving a log saved in the system according to the desired time.

Report Policy

Detail Search					
	YEAR	MONTH	DAY	HOUR	MINUTE
From	1970 ▾	1 ▾	1 ▾	9 ▾	00 ▾
To	1970 ▾	1 ▾	2 ▾	19 ▾	00 ▾

Click the **[OK]** button after setting the desired time to verify the following log below. Click the **[Reset]** button to return to the previous status.

Log Report		
[1970-1-1 9 : 00] ~ [1970-1-2 19 : 00]		
Date/Time	Message	Type
1970/1/1 9:0:33	xinetd Version 2.3.11 started with libwrap options compiled in.	xinetd
1970/1/1 9:0:33	Started working: 2 available services	xinetd
1970/1/1 9:0:36	xinetd startup succeeded	02xinetd
1970/1/1 9:0:38	Entering runlevel: 3	init
1970/1/1 9:0:41	session opened for user toor by (uid=0)	login
1970/1/1 9:0:41	toor[190] ROOT LOGIN ON console	--
1970/1/1 9:42:42	check pass; user unknown	login
1970/1/1 9:42:42	authentication failure; logname= uid=0 euid=0 tty=pts/0 ruser= rhost=192.168.0.125	login
1970/1/1 9:42:44	FAILED LOGIN 1 FROM 192.168.0.125 FOR adm, Authentication service cannot retrieve authentication info.	login
1970/1/1 9:42:46	session opened for user admin by (uid=0)	login

First Prev+10 ◀ Prev. 1/5 Next ▶ Next+10 Last

Click one of the buttons on the bottom of the window above to move the desired page. Click the **[First]** or **[Last]** button to move to the first page or last page. Click the **[Next]** or **[Prev]** button to move the previous or next page. Click the **[Next+10]** or **[Prev+10]** button to move the 10 pages backward or forward.

Download

This page allows downloading the log of the system that is currently saved. Press the **[Download]** button to download the system log in the form of a compressed file.

Log File Management	
Download log file	
To download log files	
Click the [Download] button.	
Download	

NTP Server

NTP Server synchronizes the timezone, date and time of the system on the **[Time Configuration]** menu of the **[System]** through a network or sets up the values by itself.

NTP Config

Select **[Time Configuration]** → **[NTP Config]** and set up Time Server to synchronize the information on the time server, date and time. Current Time indicates the current time of the system. NTP Server Status indicates the execution status of NTP Demon.

Time Server is registered in the Time Server table. For the registration method, both IP and Domain Name methods are available. (But, to use Domain Name, DNS Server should be set up. To synchronize with Time Server by configuring such NTP, a network should be connected.)

If registering Time Server, click the **[OK]** button to start or restart NTP demon.

NTP Configuration

Current Time		
2005. Sep. 26. (Mon) 19:13:57		

NTP Server Status	
Status	stop

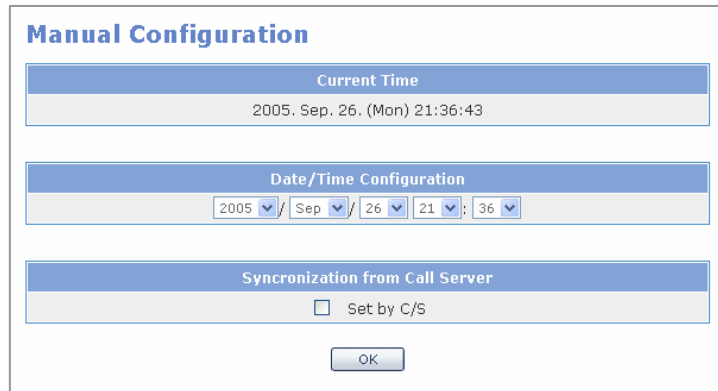
Time Server		
Server 1		
Server 2		

OK

Manual Config

This window allows setting and modifying the date and time of the system to the time that the user wants in the menu of **[Time Configuration] → [Manual Config]**. If clicking the **[OK]** button after selecting date and time that the user wants in the table of Date/Time Configuration, the date and time of the system is changed to the selected time.

Check and click the **[OK]** button to synchronize the date and time of the user from Call Server table with Call Server.

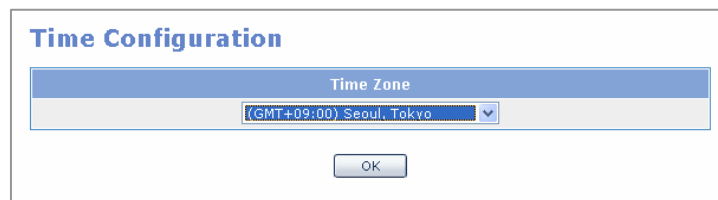


The **Manual Configuration** window contains three main sections. The first section, **Current Time**, displays the system's current date and time as '2005. Sep. 26. (Mon) 21:36:43'. The second section, **Date/Time Configuration**, provides input fields for manually setting the date and time, currently showing '2005 / Sep / 26' and '21 : 36'. The third section, **Synchronization from Call Server**, includes a checkbox labeled 'Set by C/S' which is currently unchecked. An **OK** button is located at the bottom center of the window.

Timezone

This window allows changing the timezone by selecting the timezone related to the user from the **[Time Configuration] → [Timezone]** menu.

Select the desired area(city or GMT) in the areas by GMT and click the **[OK]** button to modify the timezone information of the system.



The **Time Configuration** window features a **Time Zone** section with a dropdown menu. The selected option is '(GMT+09:00) Seoul, Tokyo'. An **OK** button is positioned at the bottom center of the window.

Upgrade

Upgrade the Kernel and Ramdisk in the **[Upgrade]** menu.

For the types of upgrade, there are 'TFTP Method' and 'File Transmission Method through HTTP' as well as Local Method that uploads the user's PC. When upgrading a package, the package version to upgrade should be entered like 'v0.19' in the 'Package Version' field.

Select Package Upgraded

Package Version	Current Version	Released Date	Upgraded Date
	v0.19	2005.09.21	2005.09.21

Select Upgrade Method

Upgrade Method	Upgrade Server IP
☒ TFTP	. . .
☐ HTTP	
☐ Local	Browse...

For TFTP/HTTP, enter the address of the TFTP/HTTP server and click the **[OK]** button. For Local method, the relevant package file should exist in the user's PC. Click the **[OK]** button after selecting the file.

In the TFTP/HTTP method, the files of the relevant version are searched automatically and downloaded, but for Local method, the entered version name and file name to upload should be identical.

If Package Version is 'v0.19', the file name is 'gsim-pkg-v0.19.tgz'.

Appl Server

The **[Appl Server]** menu manages the services of SSH, FTP and Telnet and it is available to connect to the GSIM board by using these services.

Application Server

	On/Off
SSH	☒
FTP	☒
Telnet	☒

Reboot

The user can reboot the system in the **[Reboot]** menu.

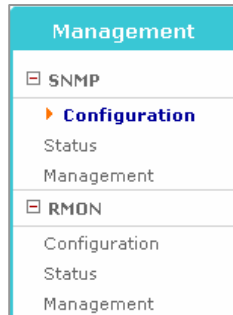


If clicking the **[OK]** button, all services are terminated and the system is rebooted.

The webscreen returns to the initial login window and the webscreen does not operate before the network and service are all executed after rebooting.

Management Menu

Select **[Management]** menu. The submenus will be displayed in the upper left side of the window as follows:



Menu	Submenu	Description
SNMP	Configuration	Displays the setup items of SNMP.
	Status	Displays the SNMP setup currently configured.
	Management	Starts/Stops the SNMP service.
RMON	Configuration	Displays the setup items of RMON.
	Status	Displays the RMON set currently configured.
	Management	Starts/Stops the RMON services.

SNMP

Configuration

[SNMP] → [Configuration]

Click the **[Save]** button to apply the setup to the system. Click the **[Reset]** button to reset the setup currently set up by the user.

System Option

Set up SNMP System Option.

System Option	
Location	
Contact	
Name	
Engine ID	

Item	Description
Location	Sets up the information on System Location.
Contact	Sets up the information on System Contact.
Name	Sets up the information on System Name.
Engine ID	Sets up the information on System Engine ID.

Community

Add the community used in SNMP v1/2c.

Community	
New Community name	
Community Network	. . . /
Access	☒ Read Only ☐ Read Write

Item	Description
New Community name	Fills in new community name to add.
Community Network	Sets up new community network to add.
Access	Sets up the access authority.

SNMPv3 User Add

This window adds a user to be used at SNMP v3.

SNMPv3 User Add	
User Name	
User Password	
Authentication	MD5 v
Encryption	None v
Access	☒ Read Only ☐ Read Write

Item	Description
User Name	Fills in new user's name to add.
User Password	Fills in new user's password. 8 alphanumeric characters
Authentication	Sets up authentication method.
Encryption	Sets up ciphering method.
Access	Sets up access authority.

Trap Manager

This window is used to set up IP address to transmit a trap. Up to five addresses can be designated.

Trap Manager	
IP Address	. . .
Community Name	

Item	Description
IP Address	Sets up new Trap IP Address to add.
Community Name	Sets up a community used to transmit to the Trap IP Address to be added.

Status

The function is used for retrieving the SNMP setup in the **[SNMP] → [Status]** menu.
 If clicking the **[Delete]** button, the item that the user has selected by marking on the check box is deleted.
 If clicking the **[Reset]** button, all check boxes are initialized.

SNMP Config Information

This window is used for retrieving the SNMP setup.

System Information			
Location	Seoul, Korea		
Contact	support@		
Name	OS7400-GSIM		
Engine ID	GSIM		

Select	Community Name	Community Net	Access
☐	private	local	Read Write
☐	public	anynet	Read Only

Select	User Name	Access
☐	root	Read Write

Select	Trap IP	Trap Port
☐	192.168.0.123	162

Item	Description
System Information	Displays the information set up at System Options.
Select	Selects information to delete.
Community Name	Displays the community name.

Item	Description
Community Net	Displays the established name of the Community Network.
Community Access	Displays the access authority of the established community.
User Name	Displays the established user's name.
Access	Displays the access authority of the established user.
Trap IP	Displays the established Trap IP.
Trap Port	Displays the established Trap Port.

Management

In the **[SNMP] → [Management]** menu, the user can start/stop the SNMP service.

If clicking the **[Run]** button, the SNMP service starts.

If clicking the **[Stop]** button, the SNMP service stops.

SNMP Management

In this window, the user can start/stop the SNMP service.

Activity	Action
Running	Stop

Item	Description
Activity	Displays the operational condition of the current service.
Action	Selects whether to start/stop.

RMON

Configuration

In the **[RMON] → [Configuration]** menu, the user can set up RMON Global.

If clicking the **[Save]** button, the information that is set up by the user is applied to the system.

If clicking the **[Reset]** button, the information that the user is to set up is reset.

History Option

Set up RMON History Option.

History Option		
MAX History Buckets	1000	(50 - 5000)
MIN History Interval	15	min. (1 - 60)

Item	Description
MAX History Buckets	Sets up the maximum history storage space.
MIN History Interval	Sets the minimum collection interval of the history interval.

Event Options

This window is used for setting RMON Event Option.

Event Option	
MAX Event Logs	(50 - 2000)

Item	Description
Max Event Logs	Sets up the maximum number of Event Logs.

Status

In the **[RMON] → [Status]** menu, the user can retrieve the setup for RMON Global. If clicking the **[Refresh]** button, the displayed information is synchronized.

RMON Global Status

This window is used for retrieving the SNMP setup.

History Global Status	
MAX History Buckets	1000
Granted History Buckets	0
Used History Buckets	0
MIN History Interval	15 min.

Event Global Status	
MAX Event Logs	400
Saved Event Logs	0

Item	Description
MAX History Buckets	Displays the maximum history storage space that has been set up.
Granted History Buckets	Displays the history storage space that is currently allocated.
Used History Buckets	Displays the history storage space that is currently used.
MIN History Interval	Sets the minimum collection interval of the history interval.

Item	Description
Max Event Logs	Displays the maximum number of logs that are set up.
Saved Event Logs	Displays the number of logs that is currently stored.

Management

In the **[RMON]** → **[Management]** menu, the user can start/terminate the RMON service. If clicking the **[Run]** button, the RMON service starts.

If clicking the **[Stop]** button, the RMON service stops.

RMON Management

This window is used to start/stop the RMON service.

RMON Management	
Activity	Action
Stop	Run

Item	Description
Activity	Displays the operational status of the current service.
Action	Selects whether to start/stop.

ABBREVIATION

A

ARP Address Resolution Protocol

B

BGP Border Gateway Protocol
BPDU Bridge Protocol Data Unit
BSR Bootstrap Router

C

CTI Computer Telephony Integration

D

DHCP Dynamic Host Configuration Protocol
DNS Domain Name Server
DVMRP Distance Vector Multicast Routing Protocol

G

GSIM Gigabit Switch Interface Module
GVRP GARP VLAN Registration Protocol

H

HTTP Hypertext Transfer Protocol

I

IGMP Internet Group Management Protocol
IPSec IP Security Protocol
IPMC IP Multicast

L

LAN Local Area Network
L2TP Layer 2 Tunneling Protocol

N

NTP Network Time Protocol

P

PIM-SM Protocol Independent Multicast-Sparse Mode
PoE Power Of Ethernet
PPTP Point to Point Tunneling Protocol
PVC Permanent Virtual Circuit
PVID Port VLAN Identification

Q

QoS Quality of Service

R

RMON Realtime Monitoring
RP Rendezvous Point
RSTP Rapid Spanning Tree Protocol

S

STP Spanning Tree Protocol
SNMP Simple Network Management Protocol

T

TFTP Trivial File Transfer Protocol

V

VLAN Virtual Local Area Network
VPN Virtual Private Network